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

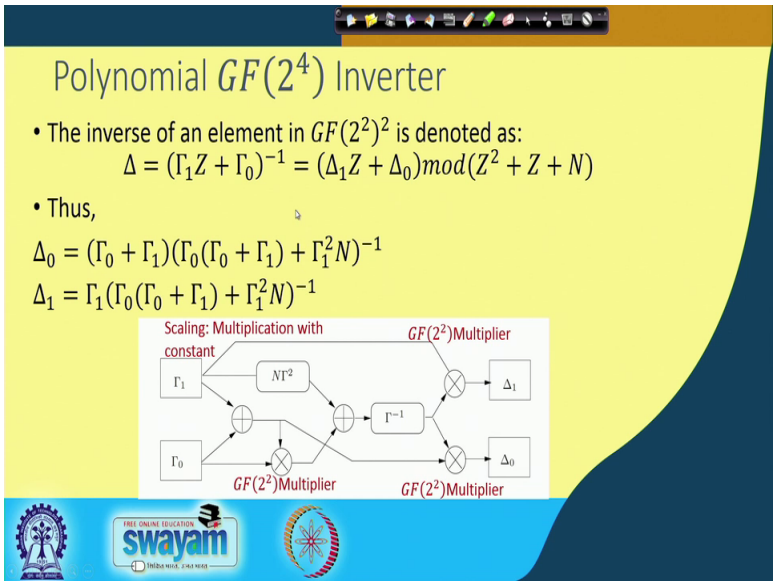
Lecture - 16
Compact AES S - Box (Contd.)

So welcome back. So, we shall be continuing with our discussions on the Compact AES S Box implementation in polynomial basis. So, we shall we were talking in the last class on the squaring and scaling operations.

(Refer Slide Time: 00:27)

So, we will be continue with that and try to see how we can eventually get the overall S box designed.

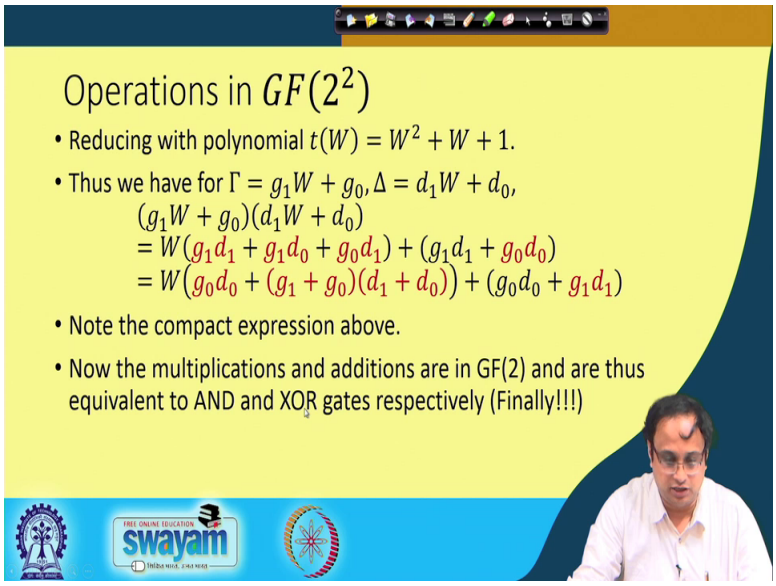
(Refer Slide Time: 00:33)



So, in order to start with right we have already seen that how we can decompose a GF 2 power of 8 circuit into GF 2 power of 4 operations. So, let us try to now take a look about how we can implement GF 2 power of 4 invert which inversion, which you remember was one of the components in my circuit So therefore, now again in a similar fashion the inverse I can again right a GF 2 power of 4 element equivalently in the field GF 2 power of 2 whole power of 2.

And therefore, right the components say delta right will be equal to suppose, delta is the inverse of gamma 1 Z plus gamma 0 whole to the power of minus 1. And the result is say delta 1 z plus delta 0, remember that when you are doing this you are doing a modulo with Z square plus Z plus N ok. So therefore, the results here are exactly like what we have calculated previously. And therefore, the circuit also is exactly similar ok, express that now expect the now these elements are in GF 2 power of 2 ok.

(Refer Slide Time: 01:39)



So, therefore, right if you want to realise this then you have got GF 2 power of 2 multipliers and the inversion is also GF 2 power of 2 ok. So therefore, right again the, so therefore, you are now doing operations in GF 2 power of 2, but if you want to when you are doing operations in GF 2 power of 2, you can again you know like decompose the element say you can right 2 when you are one multiplying. So, 2 elements, say you know like when you are multiplying 2 elements like gamma and delta, say gamma is g 1 W plus g 0, so now, again I am breaking GF 2 power of 2 as GF 2 2 whole power of 2.

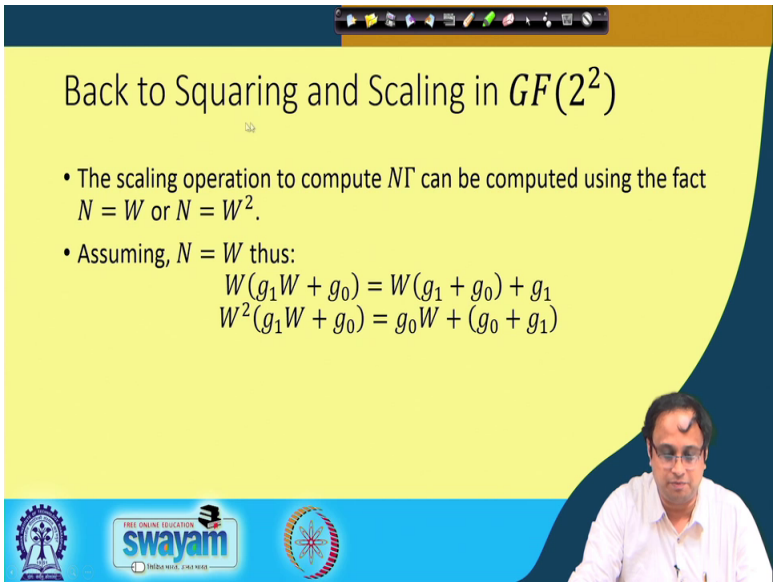
So, I can I am writing this as, so remember that the g 1 is one bit and g, so, GF 2 power of 2 I am writing as g 1 W plus g 0, which means g 1 is 1 bit and g 0 is also 1 bit there both elements from GF 2 ok. Likewise delta is d 1 W plus d 0, which means d 1 and d 0 are in GF 2. So, when I am multiplying gamma and delta; that means, g 1 W plus g 0 with d 1 W plus d 0 again remember that I will get the term like W square. So, I have to again have an irreducible polynomial. The irreducible polynomial in this case is W square plus W plus one there is only one irreducible polynomial choice ok. So, that is why right, but again you know like this equation can have two roots and therefore, you have got 2 polynomial basis choices ok.

Suppose I take one of them and let us call it as W and therefore, right I can write now these as W into as follows. So, this is my simplified expression. Note that if I do that in this fashion, I will have 4 independent multiplications, which I have coloured as in the

colour red. You can also write that in an equivalent form as shown here, but note now you have got to do three multiplications ok, like here is one multiplication, here is second one, here is another multiplication, I will be take the cost of doing more few more XORs ok.

So, note the compact expression above therefore, this is the apparently a compact we have writing it. And, but now interested we note that, the multiplications and the additions are now in GF 2; which means now they are 1 bit elements and therefore, they are nothing, but and gates and or gates ok. So finally, we write we have gone down to bits right essentially and we essentially do not need to decompose any further ok. So, now ones we have done an operation in GF 2 power of 2; that means, you know how to do a multiplication in GF 2 power of 2.

(Refer Slide Time: 03:53)

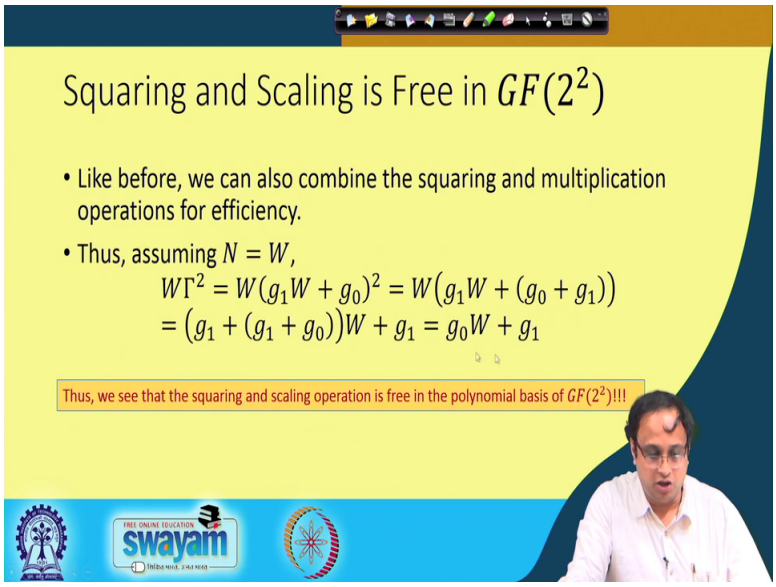


Let us get back to our squaring and scaling and see like what is the effect back ok. So, this is very interesting thing for example, you can see that the scaling operation to compute. So, let us just compute as first of all simple scaling with N and with N where you know like one of them is say N equal to W or say N equals to W square ok. So, remember that we had such kind of operations in our circuit; for example, if you go back right here is a scaling operation where you are doing with N ok.

So, therefore, it is important to know how to do that operation and a it's quite simple. So, what you can do is that, so now you have got elements g 1 W plus g 0 that is an element

in GF 2 power of 2, you are multiplying that with N equal to W. And therefore, when you multiply this you will get omega square g 1 plus g 0; remember that omega square again you can decompose like what we have seen before. Because you know that omega square equal to W, I mean that omega square W square is equal to W plus 1 and therefore, with that substitution you will get W into g 1 plus g 0 plus g 1 ok. Likewise the scaling with W square can also the represent in this fashion, we have got g 0 W plus g 0 plus g 1 ok.

(Refer Slide Time: 05:05)



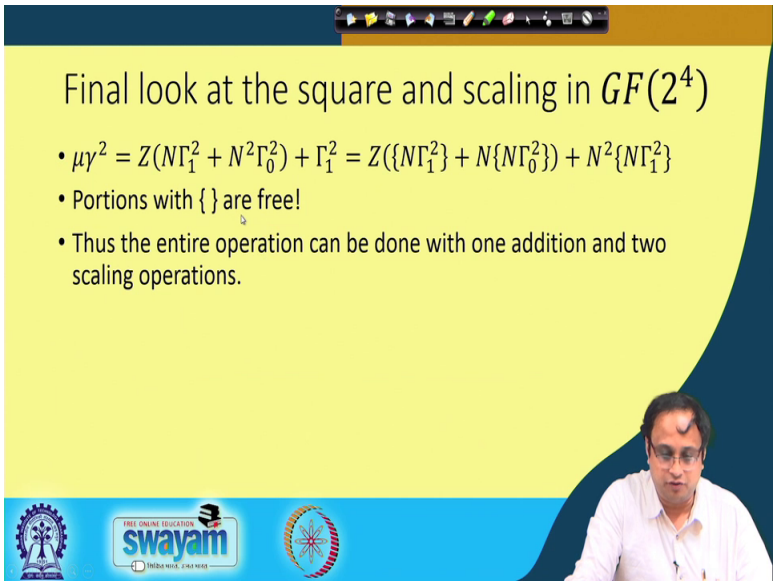
So, now when you are doing a squaring and scaling; that means, why do we you know like, now let us try to understand the importance of this circuit. Why we are doing squaring and then scaling why we are trying to combine these 2 circuits ok.

It turns out that in GF 2 power of 2 this operation is free ok. For example, what I am doing is that I am trying to do W into tau square ok. So, suppose N equal to W and I am doing W in to tau square. Then the operation that I am doing is W multiplied with g 1 W plus g 0 whole square and this write is nothing, but g 1 W plus g 0 plus g 1 ok. So, again I have substituted W square as W plus 1 and this is what I get.

So, now if I again you know like multiply W with W W, I get W square and then again I replace W square with W plus 1 and finally, right after few signification I get g 0 W plus g 1. So, you need note them input was g g 1 W plus g 0 after doing squaring and scaling I just get the same result only swapped. So, I just need to swap the higher 2 2 part the higher part with the lower part ok.

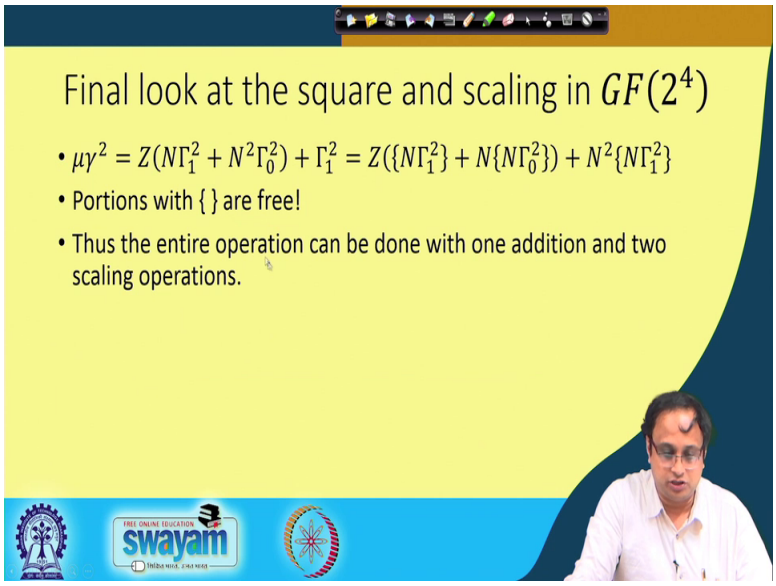
So, therefore, this result, this is a 2 bit result, this is a 2 bit value because g 1 is from GF 2 g 0 is also from GF 2 and the result right of squaring and scaling is nothing, but the swap of this bits. So, this is important note that we see the squaring and scaling operation is free in the polynomial basis of GF 2 power of 2 ok.

(Refer Slide Time: 06:31)



So, therefore, right this also has an effect on the on the bigger or you know like the top the one the squaring and the scaling in GF 2 power of 4 ok. So, if you remember right the stopped at this result where mu gamma square was equal to Z into N tau 1 square plus N square tau 0 square plus tau 1 square ok.

(Refer Slide Time: 06:31)

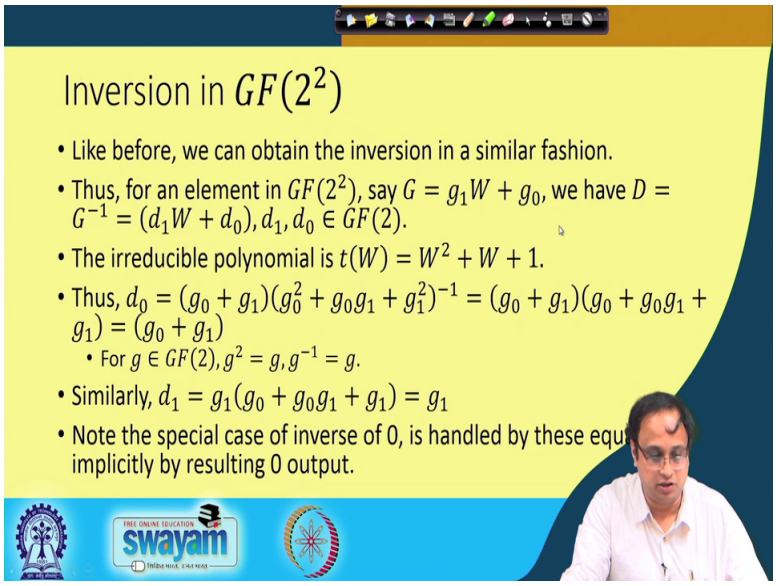


So, now if you want to take the advantage of the previous result; that is the squaring and scaling is free in GF 2 power of 2, you can actually write this N gamma one square. So, remember this is an operation in GF 2 power of 2 and now this is free. So, you suddenly observe that this operation is free and you can also write this operation as N multiplied with N gamma square.

So, like a if you do that right you just need to do one scaling operation, because the part in the parenthesis is free. Likewise gamma 1 square., you can actually write as N square into N gamma 1 square, because N to the power of 3 is 1 in GF 2 power of 2 ok, because there are 4 elements as I said. And therefore, right you essentially again have this free and you just need to do a scaling with N square and you have already discussed about the corresponding equations on how we can do scaling with both N equal to W and with N equal to W square; that means, N and N square.

So, if you just for plug in these equations, you should be able to perform these 2 scaling operations; that means, scaling with N and scaling with N square. So, therefore, the entire operation can now be done with one addition and with two scaling operations which you have already seen ok.

(Refer Slide Time: 08:07)



So, finally, right you have you have one more step to be observe, which is like the inversion in GF 2 power of 2 like before we can again obtain the inversion in a similar fashion. Therefore, if you take an element g 1 W plus g 0, which is an element on GF 2 power of 2 and if you want calculate capital D, which is the inverse of g then D is equal to d 1 W plus d 0 ok, which is a inverse of g which is g 1 W plus g 0.

So, therefore, again when you are doing is the operations remember that your irreducible polynomial will be the irreducible polynomial of this decomposition which is W square plus W plus 1. So, you are basically writing your GF 2 power of 2 element now in terms of GF 2 elements and the corresponding irreducible polynomial is W square plus W plus 1.

So, therefore, right if I again apply the equations which you have seen in the previous case and just because essentially nothing changes express the, except the variable names. So, if you just use the same equations you get d 0 which is equal to g 0 plus g 1 into g 0 square plus g 0 g 1 plus g 1 square whole to the power of minus 1 ok. But, note that this element is now a GF 2 element and in GF 2 which means either it is 0 or one the inverse of 1 is 1 and the inverse of 0 we define as 0 ok.

So, with that definition, I can actually replace or just neglect this minus 1 or neglect this 2 to the power of minus 1 and rather calculate these are g 0 plus g 1 into g 0 plus g 0 g 1 plus g 1 and this turns out to be g 0 plus g 1. So, what we have trying to say here is that

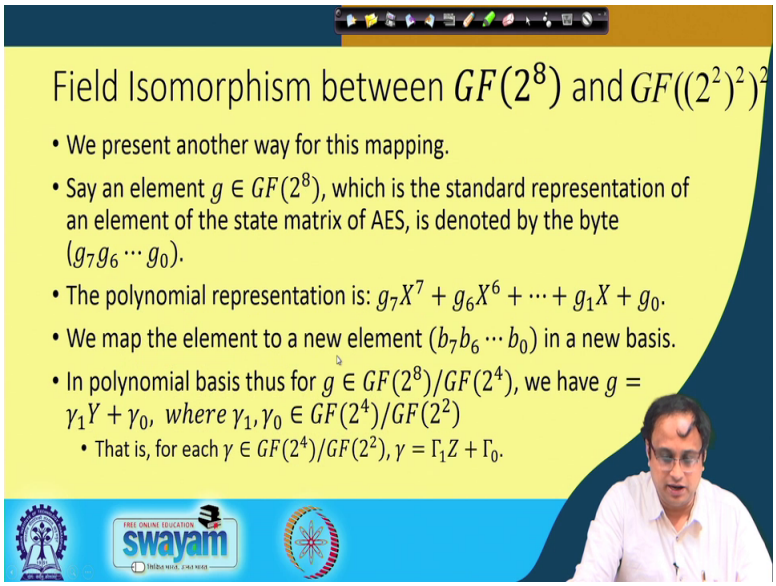
for any non 0 GF 2 element; that means, suppose it is 1, then I can write g square as g and likewise I can also write g to the power of minus 1 as g ok.

So, therefore, with this simple observations right I get d 0 as g 0 plus g 1 and likewise my d 1 is also equal to g 1 into g 0 plus g 0 g 1 plus g 1 to the power of minus 1, but I can neglect that minus 1 in a similar way. And therefore, I get only g 1 ok. So, if you observed like g 1 into g 0 plus g 1 square g 0, so that g 1 square will become g 1. So, I will get g 1 g 0 plus g 1 g 0, remember these are all additions in GF 2 field, so therefore, it is the XOR.

So, therefore, these 2 will cancel. So, I will have got g 1 square which is equal to g 1 ok. So, note the special case of the inverse of 0 is handled by these equations implicitly, because if my input is 0 my output is 0 ok, like if I plug in input say d 1 W plus d 0. And I want to calculate the, I mean if I want to calculate say the inverse of g 1 W plus g 0, where both g 0 and g 1 are 0 ok.

So, if you plug into these equations, you are d one will be equal to g 1 which is 0 and d 0 is equal to g 0 plus g 1, since both of them are 0 you still get 0 ok. So therefore, this equations implicitly tackles your special case of 0 inverse being 0 ok, for other cases also it correctly calculates.

(Refer Slide Time: 11:17)



So, therefore, right finally, we have you know like kind of understood the underlying field operations. Now we need to put them together ok. So, remember that what will be doing is, we will be first of all realizing the top most circuit in GF 2 power of 8 and then all the underlying operations we will be essentially doing by the equation that we have studied till now. One thing we need to still discuss is about the field isomorphism between GF 2 power of 8 to GF 2 power of 2 power of 2 ok.

Of course you have seen few techniques in the previous class. In candidates paper there was a very nice technique which you can also adopt here. So, what we can do is that, we can rather take an element g which is say an element in GF 2 power of 8, which is the standard representation of an element of the state matrix of AES and it is denoted by the byte g 7 to g 0 ok.

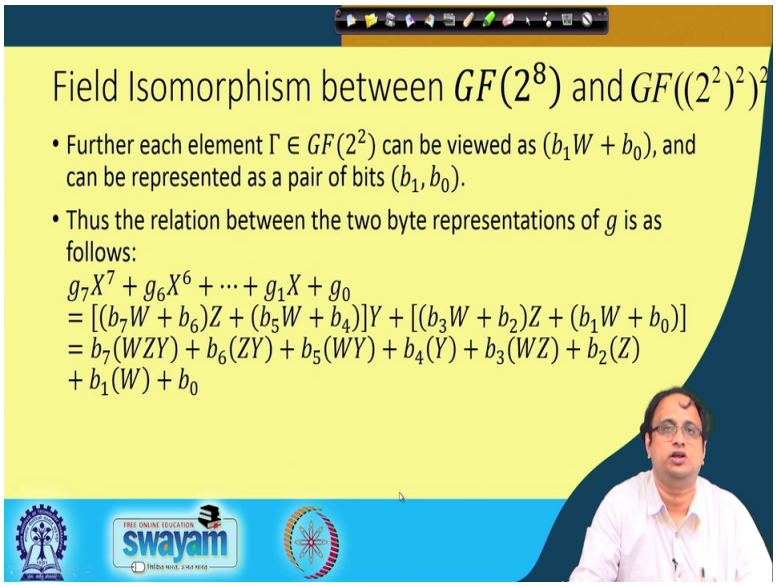
Now, the polynomial representation for this element in G F 2 power of 8 is therefore, g 7 X to the power 7 plus so on till g 0. So, note that all these elements like g 7, g 6 and so on till g 0 are all elements in GF 2; that means, either g 0 or 1. So, if you want to map this element to a new element in a new basis. So, this again will be have an 8 bits in the vector because the mapping has to be 1 to 1, so it has to be equinumerous. So, again I will get b 0 to b 7, but interestingly we need to understand the transformation of the transformation function from b 0 to b 7 in terms of g 1 to g 7 and vice versa.

So, in polynomial basis therefore, right when you are expressing you know like G f 2 power of 8 in G F to power of 4 square. So, I consider this quotient field. So, therefore, right in this quotient field what I am trying to do is that I am trying to basically simply write g as gamma 1 y plus gamma 0, where each of this gamma 1 and gamma 0 are elements in GF 2 power of 4, but again that is also written as GF 2 power of 2 whole power of 2 ok.

So, therefore, we are trying to do this in a recursive fashion. Therefore, each of this gamma can also be intern expressed as capital gamma 1 Z plus capital gamma 0 ok. So, to summarize what I am trying to say is that you are trying to express this polynomial basis polynomials representation in GF 2 power of 8 in terms as you know like g being equal to gamma 1 y plus gamma 0. Where, each of this gamma 1 can be or each of this gamma as like a gamma 1 and gamma 0 can be expressed as you know like capital gamma 1 Z plus capital gamma 0 ok.

So, likewise right remember that these are now element in GF 2 power of 2 ok.

(Refer Slide Time: 13:53)

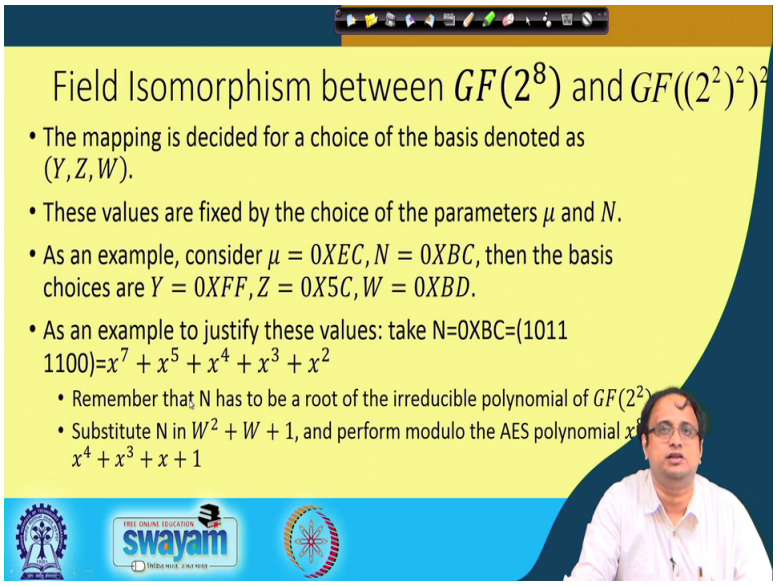


So, therefore, you can further write it as b 1 W plus b 0, where each of this b 1 and b 0 are elements in GF 2 and therefore, there nothing, but bits single bits ok. So, therefore, equivalently you can write this polynomial as 2 parts: The first part is this where the you know like the wherein have been it is y and the lower part is the constant ok. Again the lower part you can decompose into two parts, the first part again will have z as a in determinate and the lower part will be constant ok.

So therefore, it will be something like b 3 W plus b 2 into Z plus b 1 W plus b 0; likewise the top part that is the you know like b 7 to b 4, you can arrange that as b 7 W plus b 6 Z. So, this is the independent is Z and in the and the corresponding constant term is b 5 W plus b 4 ok. So, therefore, if you now kind of you know like sort of simplify this and elaborate this you will have b b 7 the b 7 will be like multiply with W Z and Y.

So, you will get W Z Y here; likewise for b 6, you will get Z multiply with Y. So, it is Z Y here and for b 5, you will get W with y. So, you will get W y here and with b 4 you will get only Y. What about the lower parts? So, b 3 will have a term W and W Z. So, you will get W multiplied with Z. For example, for b 2, you will have only Z, for b 1, you will have W and b 0, it is a constant term.

(Refer Slide Time: 15:35)



So, therefore, like the mappings you can actually elaborate them in the form of a matrix. So, what I mean is that if you want to convert say g seven to in an and you want to get you know like the corresponding elements you want to get the corresponding mappings, then you need to know these values, you need to know the values of say W z y z y and so on ok.

So, how do you get these values? So, as I said that we start the you know like the mapping is decided for a choice of the basis, which is denoted as Y Z W. So, remember that Y is my polynomial basis for GF 2 power of 4 square and Z is my polynomial basis for when GF 2 power of 2 and W is my polynomial basis when i am expressing in terms of GF 2 ok. So, these values are fixed by the choice of the parameters mu and N ok. And as you have discuss right mu, mu is to satisfy some criteria, N is to satisfy some criteria. So, here of some choices which was proposed in (Refer Time: 16:31) paper. So, remember that I can also express them as are GF 2 power of 8 element.

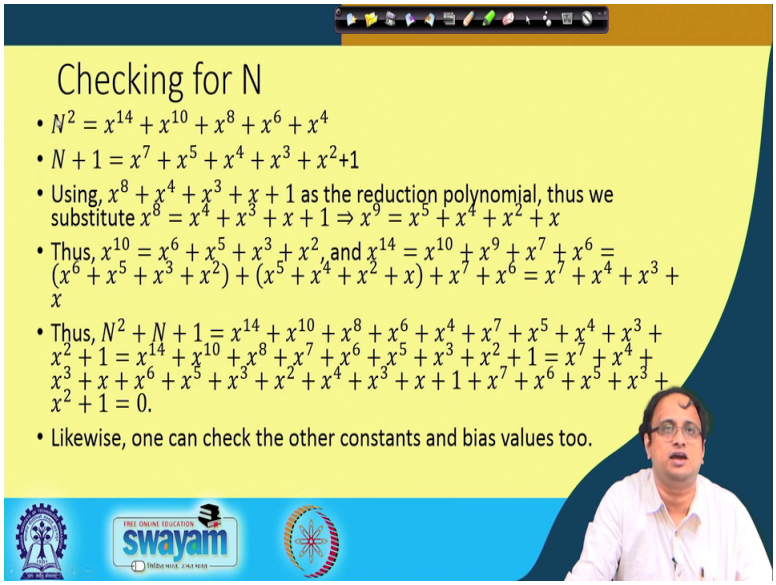
So, therefore, I express mu as the in a hexadecimal notation I express that E C N, I express as the B C and if you use this and solve the first suppose I take this value of mu then, I get my equation of the topmost polynomial becomes Y square plus Y plus mu. And therefore, if you solve it right, you should get a value of Y, which is say 0 x f f ok. Likewise for Z square plus Z plus N, if you solve you will get 5 C as a value for Z and

likewise if you solve W square plus W plus 1, one of the choices is B D ok. For other choices you will have other circuits.

Let me as an example explain the choice of N, like I said that suppose N is equal to 0 XBC, so if you want to write BC, you can express B C as 1 0 1 1; that is your elaboration for b in binary and likewise d is nothing, but 1100. So therefore, right this polynomial, if you want to express this as a GF 2 power of 8 polynomial, this is nothing, but x to the power of 7 plus x to the power of 5 plus x to the power of 4 plus x to the power of 3 plus x square ok.

So, remember the choice of N has to be such that it has to be a root of the irreducible polynomial of GF 2 power of 2; that is why how we were essentially choosing N right, N has to be a root of the irreducible polynomial of GF 2 power of 2 and the corresponding polynomial was W square plus W plus 1. Therefore, N has to be a root of W square plus W plus 1. So, let us verify this and when you do this, write will always be performing modulo with the AES polynomial which is x to the power of 8 plus x to the power of 4 plus x cube plus x plus 1 ok.

(Refer Slide Time: 18:21)



So, here is a simple verification of that, I take N square. So, N square right is nothing, but the square of N. So, this is my N. So, if I square it, everything will get powers of 2 because again I am doing a characteristic do operation. So, I will get a x to the power of 14 plus x to the power of 10 plus x to the power of 8 plus x to the power of 6 plus x to

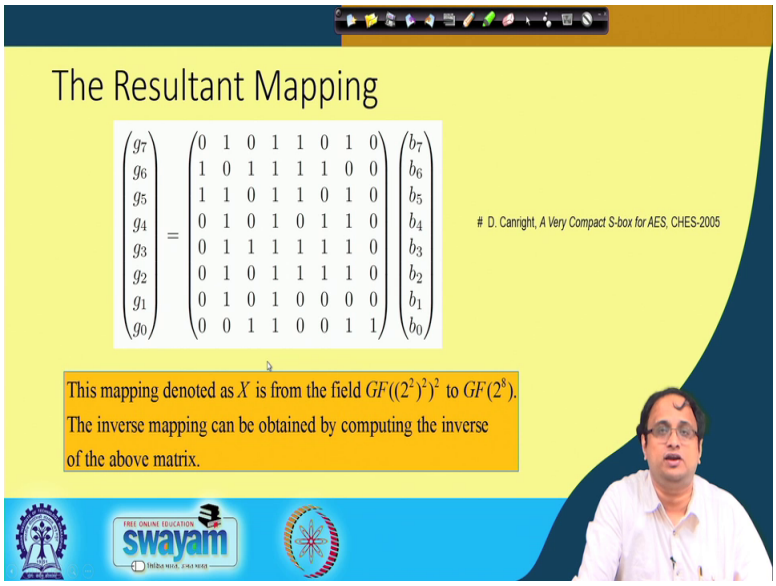
the power of 4. So, note that N plus 1 is nothing, but x to the power of 7 plus x to the power of 5 plus x to the power of 4 plus x to the power of 3 plus x squared plus 1 ok.

So, if I use this AES irreducible polynomial as my reduction polynomial, thus if you substitute x to the power of 8 as x to the power of 4 plus x to the power of 3 plus x plus 1 and if I multiply x 1 both sides again x to the power of 9 as x to the power of 5 plus x to the power of 4 plus x square plus x and again if I multiply x. Therefore, I get x to the power of 10 as x to the power of 6 plus x to the power of 5 plus x cube plus x square and now, if I want to calculate x to the power of 14 right, I can multiply x to the power of 10 ok. So, therefore, this is my I essentially want to calculate say x to the power of 14 and x to the power of 14 essentially turns out to be x to the power of 10 plus x to the power of 9 plus x to the power of 7 plus x to the power of 6 ok.

So, note that, when you are doing this operations right, I am always doing an I am reducing via this polynomial ok. So, this is my irreducible polynomial which I am using to you know like take modulo operations. So, therefore, now you know like when I when I when I want to sort of you know like reduce x to the power of 10. Therefore, I will plug in this elaboration of x to the power of 10; that is x to the power of 6 plus x to the power of 5 plus x to the power of 3 plus x square x to the power of 9 is x to the power of 5 plus x to the power of 4 plus x square plus x and this is what I plug in here.

And I have of course, got x to the power of 7 plus x to the power of six, if I simplify this turns out to be x to the power of 7, plus x to the power of 4, plus x cube plus x. If I just go ahead and calculate N square plus N plus 1, of course, I have to do few ugly operations here, but interesting rewrite if you elaborate this then all these terms will get cancelled out. And finally, you will get 0 to prove that indeed N square plus N plus one is 0, which means that you know like that N is correct choice the N that you have chosen is correct. So, likewise one can check the other constants and the bias values too.

(Refer Slide Time: 20:55)



So, therefore, the finals of step is this that now once you have this g we have got this values write as we have say as we have seen, so we need to calculate these values like you know like W Z Y, Z Y and so on and each of them will give you individual columns of your matrix. So, you see you have got 8 components here say for example, W ZY will have a corresponding value and so on everything will have you know like you can calculate this individual values.

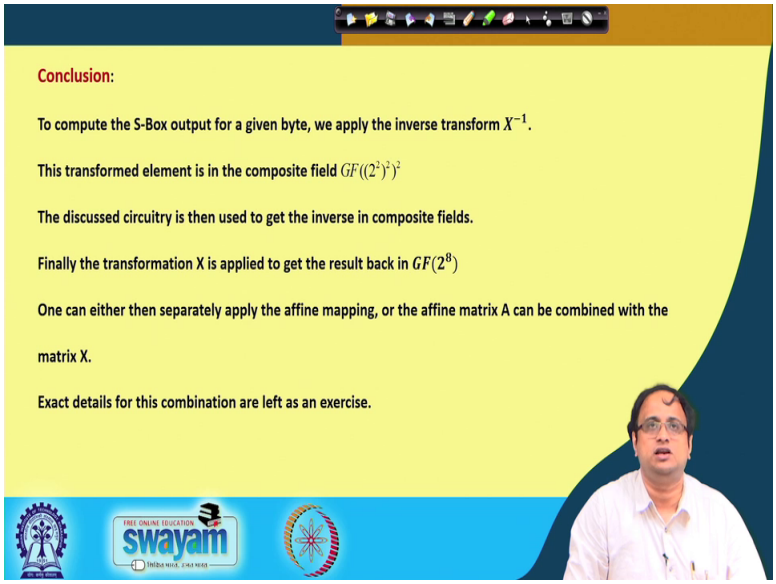
And if you if you calculate them right then each of these columns will stand for the corresponding values ok. For example, this one will stands for say W Z Y and so on ok. You can observed the last column is one and that also you can verify here that you know like in your elaboration in the last column is nothing, but 1. So, therefore, you know like b 0 is multiplied with one and therefore, you know your last column of this matrix is 1; that means, 1 gets mapped in to 1.

So, this mapping is denoted as x in the form of the field this is a mapping from G F you know like because you have you have got this has input and your calculating this has a output. So, remember this element in GF 2 power of 8. So, your basically translating GF 2 power of 2 power of 2 ok. GF 2 power of 2 whole power of 2 whole power of 2 2 GF 2 power of 8 and the inverse mapping of x; that is x inverse can be can help you translate from GF 2 power of 8 to this composite field ok.

(Refer Slide Time: 22:29)

So finally, right what we have seen is essentially also elaborate and taken from you can refer to this text book for more details on how this implementations work.

(Refer Slide Time: 22:39)



And essentially write conclude what we have discussed is we have discussed about how to compute the x box output for a given byte we apply for that the inverse transformation which is x to the power of minus 1. And this transformed element is therefore, in the is in the composite field which is GF 2 power of 2 whole power of 2 whole power of 2 and the discussion circuit is circuitry is the news to get the inverse in composite fields. And

finally, the transformation that is x we have been the transformation x is applied on the result to get the result back in GF 2 power of 8.

So, one can either separately apply then you are affine mapping or you can try to combine the affine matrix with the matrix x. Remember that in affine mapping also you have a matrix, you can try to combine that with the matrix x, but exact details of which I am not kind of formulating in my class, but rather leave as an exercise ok. So, let me stop here.

Thank you all for your attention.