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

**Lecture – 17**
**Compact AES S – Box in Normal Basis**

So, we shall continue our study on the Hardware Security class. So, we shall be continuing our pursuit to find out the efficient and compact AES S-Box. In particular in the last class, we were talking about polynomial basis representation. So, we shall be continuing to look into the normal basis domain. Try to see that whether is the normal basis domain, we have more opportunities of optimization.

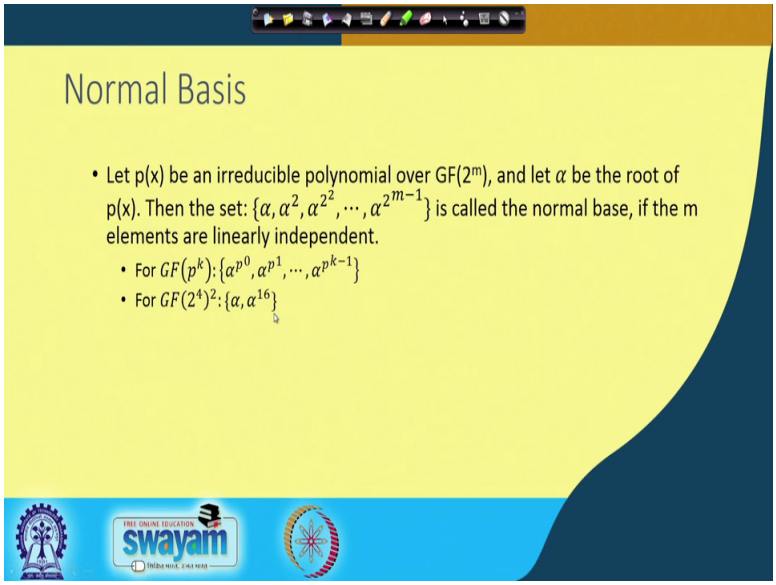
(Refer Slide Time: 00:39)


So, in today's class what I will try to cover up is essentially try to work out the circuit optimizations that we were trying to see in context of polynomial basis for normal basis. We shall be trying to look into the normal basis inverter in GF 2 power of 8. Considered the scaling and squaring operations and optimizations, which were seeing the polynomial basis again work them out in the normal basis.

We shall be trying to understand the about the hierarchical decompositions in normal basis GF 2 power of 8, GF 2 power of 4, and finally GF 2 power of 2. And finally, obtained end to end mapping for getting you know the functional equivalent output as

that of an AES S-Box. And we shall also we concluding with some finer points and comparisons with the polynomial basis representation.

(Refer Slide Time: 01:31)



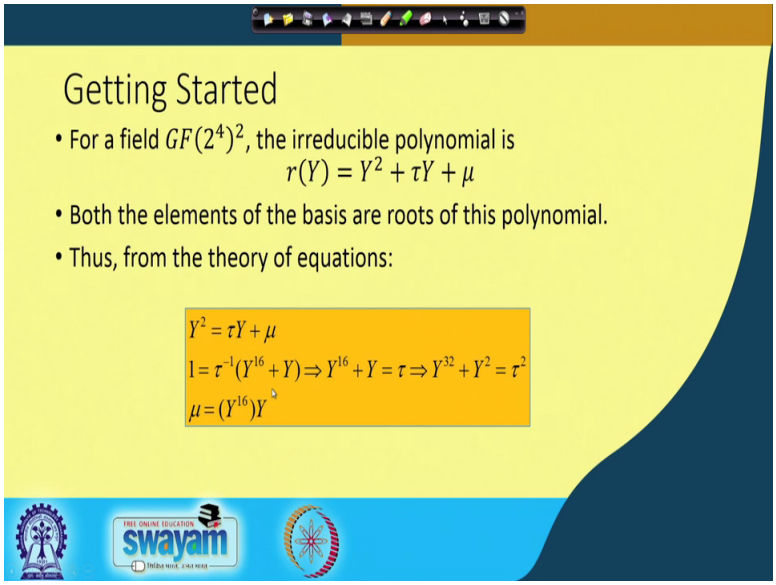

So, with this sort of idea, let us start. So, let us is just quick recap about the normal basis. So, in the normal basis representation again we have an irreducible polynomial, typically denoted as p x which is defined over the Galois field GF 2 power of m, and suppose alpha is a root of these polynomial p x. Then the set which is like denoted as alpha, alpha square, alpha to the power of 2 power of 2 and so on till alpha to the power of 2 to the power of m minus 1 is called as the normal basis.

If the m elements are linearly independent that means, for GF 2 power of GF p power of k, we can easily understand that I mean we can generalize it for GF p power of k, where you should be alpha to the power of p power of 0, alpha to the power of p power of 1, so until alpha to the power of p power of k minus 1 ok. So, you can easily understand the relation, you can plug in p equal to 2 between this and this.

And likewise write if you so this is another I mean, we will be considering composite fields like what we are doing in polynomial basis. So, we will encounter fields of this type right GF 2 power of 4 square that means, there are two parts in this argument, each of them has got are elements of GF 2 power of 4.

So, in this particular representation, the basis or the normal basis would be represented as alpha and alpha to the power of 16 ok. So, essentially this would be my basis for GF 2 power of 4 square. Likewise for GF 2 power of 2 my basis would be omega and omega power of 4 ok. So, essentially and finally when we go down to GF 2 write essentially to the lower basis, then we will find out that the basis will be denoted as say omega and omega square ok. So, we shall be seeing you know like in more details about how to use and manipulate these basic elements in our discussions.

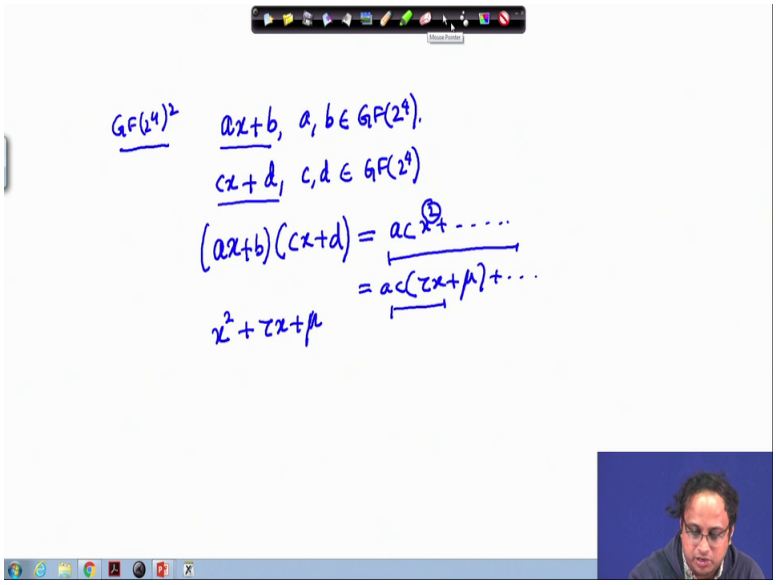
(Refer Slide Time: 03:26)




So, getting started. This is my field or starting field like I have taken a Riemann in GF 2 power of 8, and converted it into the composite field denoted as GF 2 power of 4 square. And I have used the irreducible polynomial like in the last class, so this is polynomial is r Y, which is equal to Y square plus tau Y plus mu ok.

So, therefore tau and mu are my variables, and this is my polynomial that means, if I take any two elements in the in this field, which is a GF 2 power of 4 whole square, so that means I can take any element and that element would be denoted as ax plus b ok, so that means if I just quickly try to work out you know like an element here.

(Refer Slide Time: 04:12)




Like, suppose I take GF 2 power of 4 whole square that means, this is my you know like corresponding field and I take an element for this field, and denoted as ax plus b, so that means a and b both belongs to GF 2 power of 4 ok.

So, likewise I can take another element in the field, and denoted as a cx plus d, so c and d are again elements from GF 2 to the power of 4. And if I consider a product, so this is again you know like I am considering or writing this element in the polynomial basis in the last like in the last class. So, then essentially if I multiply them that means, if I multiply ax plus b with cx plus d, then I will get elements which are like ac x square plus so on right. So, note that this now no more in this field GF 2 power of 4 square, because I get a degree which is 2 ok.

So, therefore here comes the purpose of my irreducible polynomial. So, my irreducible polynomial, I said was x square plus tau x plus mu ok. So, therefore what I will do is that in order to reduce this, I will substitute instead of a x square, I will substitute x tau x plus mu ok. So, you can easily understand now my degree is in x, so therefore this being gets back into the composite field ok.

Of course, for normal basis you have to do slightly a different type of manipulation, but the basic idea is the same ok. You have to rewrite the result back in your basis ok, so you have to write it back in your original basis ok. So, with this background I mean we can again you know like get back to this discussion.

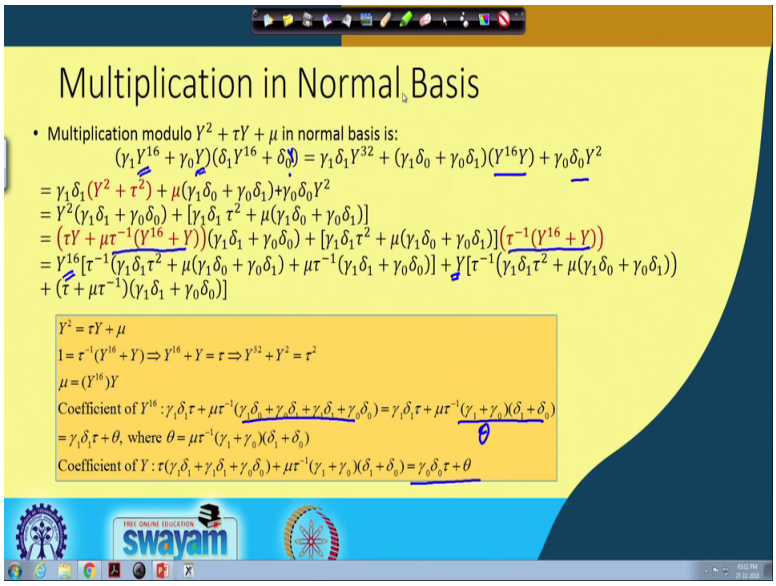
So, in so let us get back let us to now try to talk about the normal basis representation. So, in the normal basis representation interestingly, you still have the same equation which is Y when you are doing a reduction, you are writing instead of Y square, you writing tau Y plus mu. But, interestingly you see as I said probably if you remember like that the basis in this case is Y power of 16 and Y ok.

So, therefore the basis for GF 2 power of 4 whole square representation is Y power of 16 and Y, so that means I will represent an element in this field now unlike your polynomial representation, which was say ax plus b. Now, we will write it as a Y to the power of 16 plus b Y, because Y to the power of 16 comma Y is my basis ok. So, therefore I will write it as Y a Y to the power of 16 plus b Y that will be my representation in the composite field.

So, now you can note that, that means that Y power of 16 and Y, both are elements of these irreduce or both the roots of these irreducible polynomial ok. So, now if both of them are roots of irreducible polynomial that means, from the theory of equations you know that the sum of the roots that is Y power of 16 plus Y will be equal to tau will be so in this case plus and minus are same, because it is in GF 2 arithmetic.

So, therefore we can write that we can instead rewrite this as 1 is equal to tau, tau inverse Y power of 16 plus Y. That means Y power of 16 plus Y is equal to tau or we can also write just squaring both sides Y power of 32 plus Y square is equal to tau square ok. So, these are some manipulation that we will be using in our future simplifications. The other important thing is a product. So, use mu power of Y power of 16 into Y and that is equal to mu, because these stop ok. So, therefore the product that if products are the roots Y power of 16 and Y is equal to mu ok.

(Refer Slide Time: 08:01)




So, now let us consider you know like a multiplication in the normal basis ok. So, so this you can actually understand I mean if you just ignore the you know like the scribbling on the slide, and just concentrate on the problem ok, so it is not very complicated.

So, for example like let me consider let me consider two elements in the field GF 2 power of 4 whole square. So, note that one of the elements is gamma 1 Y power of 16 plus gamma 0 Y ok. So, you note that how your representing the element unlike your polynomial basis representation, because here Y power of 16 and Y are my basis. So, I have to express is express it in that basis. Unlike in the polynomial basis, my basis was x comma 1.

So, therefore I had expressed it using the (Refer Time: 08:49) x and 1 ok. So, here I have to express it using Y power of 16 and Y. And therefore, the two components are again gamma 1 and gamma 0, where gamma 1 belongs to GF 2 power of 4, and gamma 0 also belongs to GF 2 power of 4 ok. So, now so if you multiply this with another element, which is say delta 1 Y power of 16 plus delta 0.

So, now you can easily understand if we multiply, then I will get Y power of 32, because Y power of 16. And Y power of 16 will get multiplied, so I will get Y power of 32 here. And the other terms will be gamma Y power of 16 into Y, and that is gamma 1 delta 0 plus gamma 0 delta 1 Y power of 16 into Y plus term gamma 0 into gamma 0 so missed

out Y here, so please add a Y here ok. So, there should be a Y which is added here ok. So, let me just try to do the correction here ok.

So, we should actually add a Y here ok, so there should be a Y here. And therefore, write I get this term as Y power of 16 into Y, and this term as Y square, because here this and this gets multiplied ok. So, therefore I get gamma 0 into delta 0 Y square. So, now we have to do again bring the result back into the original basis, so because you note that I have got Y power of 32, I have got Y power of 16 into Y and Y square ok, none of these are basis elements.

So, therefore I what I do is I replace Y power of 32 as Y square plus tau square using the equation that we have just now seen. And Y power of 16 into Y, we can write that is mu ok, so that is my mu. And likewise have got gamma 0 and the delta 0 into Y square ok, this is still not in my basis ok.

So, therefore what I do, because mine basis is Y power of 16 and Y, so I have to bring the result back in Y power of 16 and Y ok. So, it is slightly more involved than the polynomial basis, but it can be easily understood. What if what I do is that, now I write this is in two parts. One is where I have got the Y square part ok, so the Y square in this is in multiplied with gamma 1 delta 1 plus the other term is gamma 0 into delta 0. So, this I write in one part and the other part is a constant term ok.

So, now I do a trick. So, the trick is I replace Y I replace 1 wherever there is constant, and I replace 1 using my simplification, which I have just now seen. And that is nothing but writing that has tau inverse multiplied by Y to the power of 16 plus Y ok. So, therefore right what I do here is that I take these terms ok, and I write Y square as tau Y plus mu ok, but I do not write only tau Y plus mu, but I right tau Y plus mu into 1 and one is nothing but tau inverse multiplied by Y power of 16 plus 1 ok, so that is essentially this part of the equation ok.

So, then the other part is this part that is gamma 1, delta 1, tau square plus mu, and so on. And then again this I multiply this by 1, so I write that is tau inverse multiplied by Y to the power of 16 plus Y. So, now you note that all the indeterminate that I have got are involving only Y and Y power of 16, and therefore that is my basis ok.

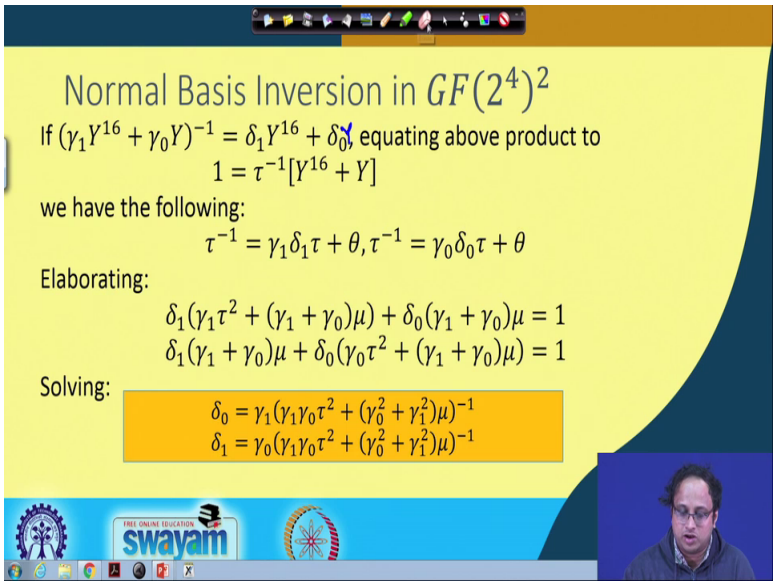
So, now if I just expand this, then I get terms which I have which are involving Y power of 16 and Y. And therefore, right I have re-written my result back in my normal basis ok. I started with my basis Y power of 16 and Y, and I have got the product also expressed in the same basis ok. So, therefore these are my two parts that mean this is my the first part, and this is my lower part ok.

And therefore, the corresponding results essentially stands for my two components of my result, you can actually make some more simplification. For example, the coefficient of Y power of 16 is written here as you know like if I just multiply for example tau inverse with tau square, I will get tau so that is gamma 1 delta 1 tau plus mu tau inverse with this part, which is gamma 1 delta 0 plus gamma 0 delta 1, this is this part ok. And then I added with you know like this part that is I just keep on doing the same thing, and I have got mu tau inverse. So, I can take mu tau inverse common from here, and I have got this is gamma 1 delta 1 plus gamma 0 delta 0 ok.

So, now you can actually you see that this can be rewritten as gamma 1 plus gamma 0 into delta 1 plus delta 0, so this you can you know like this part you can simplify as here ok. And therefore, you get the final result which you can simply denote has gamma 1 delta 1 tau plus theta ok. And this theta is nothing but this part that is essentially this is your theta ok.

So, likewise the coefficient of Y can also be interesting rewritten as this part and I am not going to the details, but I leave it to verify for you to verify the details. You can write that has gamma 0 delta 0 tau plus theta, these are the two components of my corresponding result ok.

(Refer Slide Time: 14:12)




So, now you know like with this with this right, we can actually derive the inverse equation ok. So, let us see how we can do that. So, so now once we so the when I want to derive the normal basic inversion in GF 2 power of 4 square, my basic technique will be same as that I did for polynomial basis ok.

So, now I will write this result as delta 1, Y power of 16 plus delta 0. Note that I have again so I again have for actually done my mistake here which is the basis right is Y, so therefore the Y should be here ok. This is something that we have to be always careful ok, because the basis is something irregular compare to the polynomial basis.

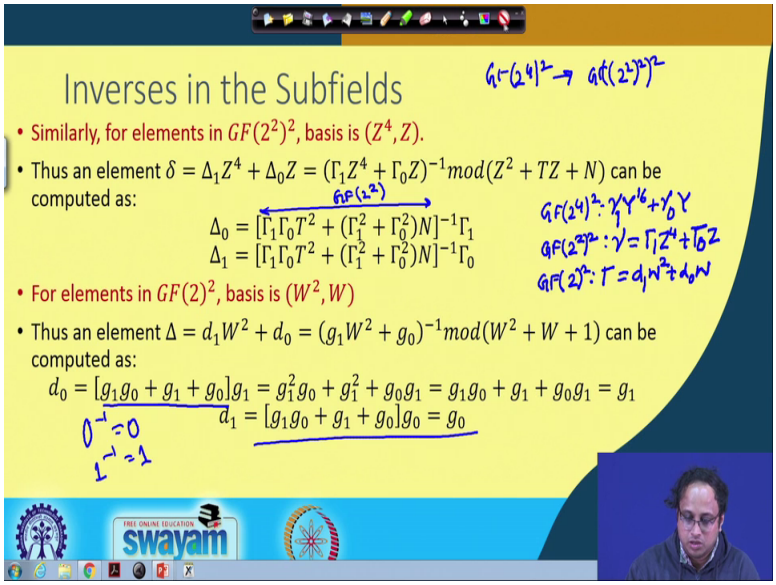
So, therefore right the result is essentially you know like so basically when I am trying to do when I am basically you know like trying to whether when this inverse relationship is satisfy that means, when I multiply this polynomial with this polynomial, I get 1 as a result ok.

And therefore, right equating the above product which I just now derive for the multiplication of two inputs to 1 ok, then 1 is nothing but tau inverse Y to the power of 16 plus Y ok. So, therefore, I can actually match the coefficients of Y power of 16 and I can match the coefficients of Y separately ok. And therefore, right what will happen is tau inverse that is tau inverse, which is the coefficient of Y power of 16 will be equal to gamma 1 delta 1 tau plus theta ok, and tau inverse will also be equal to gamma 0 delta 0 tau plus theta, these are two parts ok.

So, therefore right now if I elaborate this, and I do a little bit of simplification, then I can expressed the result delta 0 and delta 1 kind of in a similar way as that as what you have done in the context of polynomial basis ok. So, therefore finally right you can simplify these eliminate and essentially to solve the simultaneous equation to get your result delta 0 and delta 1 in this form ok.

So, you can note here that there is an inversion, which you are doing right now. If you want to get the delta 0 and delta 1 outputs, but this inversion is now in GF 2 power of 4 ok. So, therefore you have basically expressed a higher dimension inverse in terms of a smaller dimension inverse, and that is essentially the trick which we have also done for polynomial basis, and we have trying to adopt that for normal basis as well ok.

(Refer Slide Time: 16:28)




So, therefore right we basically now we can actually you know like do a similar thing for the GF 2 power of 4 inverse also. So, the GF 2 power of 4 inverse, we will know express it as a GF 2 power of 2 whole power of 2 element, but the normal basis now will be Z power of 4 comma Z ok.

So, therefore I will take elements say you know like gamma 1 Z to the power of 4 plus gamma 0 Z. So, this gamma Z capital to denote that they are in they are essentially in the base field ok, and then I do a whole power of inverse, but my polynomial is now says Z square plus T Z plus N ok. So, again you can observe that I can write my delta 0 and delta 1 in a similar fashion, but these inversions now are in GF 2 power of 2 ok.

So, therefore what I can do is now, I can write this GF 2 power of 2 as GF 2 whole square ok. So, therefore I can decompose this further, and my basis is now omega square comma omega and W square comma W. And therefore, the inverse of g 1 W squared plus 0 g g 0 whole inverse is essentially nothing but d 1 W square plus d 0, but the polynomial is done modulo of the irreducible polynomial W square plus W plus 1 ok.

So, basically right what I am trying to do again is kind of similar to what we have done previously is to express an element in GF 2 power of 4 whole square in terms of GF 2 power of 2 whole power of 2 whole power of 2 ok, so that is essentially my final objective ok.

So, therefore right what I am trying to do is that if you see the representations, when I am trying to write an element in GF 2 power of 4 whole square ok, then my element was in the form of gamma Y power of 16 plus or I can write here as a gamma 1 and gamma 0 Y ok. Likewise when I am writing it in GF 2 power of 2 that means where I am expressing GF 2 power of 4 as GF 2 power of 2 whole power of 2, then I am writing a gamma which is an element in this field as gamma 1 Z to the power of 4 plus gamma 0 Z ok. So, these are essentially these my decomposition that I am doing.

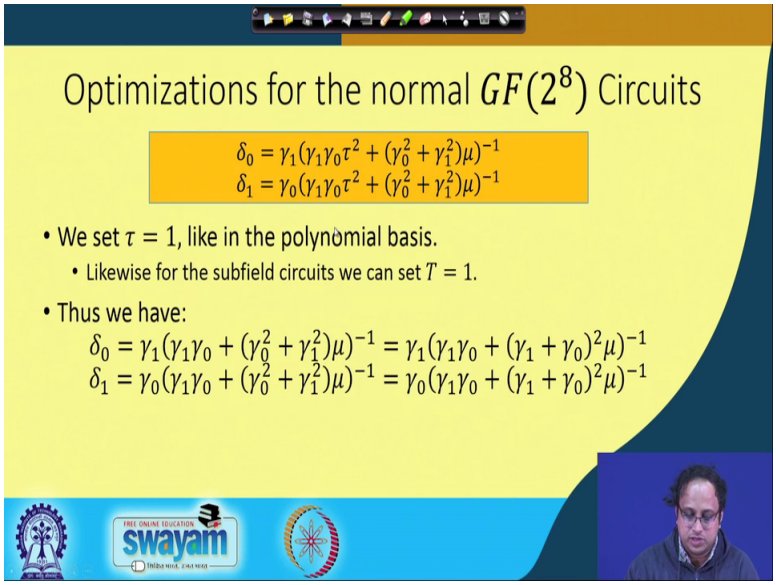
And likewise when I am writing this as GF 2 whole power of 2, then I am taking one of these capital gammas and I am writing this as d 1 W squared plus d 0 W ok. So, therefore these are my corresponding field elements. And I have to do them do this operation with respect to the corresponding irreducible polynomials ok, so that is the whole idea.

So, therefore right you can observe that this is my inverse in GF 2 power of 2 whole power of 2, where these inverses or the smaller inverses are now in GF 2 power of 2 ok. But, if you rewrite again you if you do the same thing for the smaller field now, then again you will have inverses, but these inverses are in GF 2 ok. And in GF 2 the inverse any elements inverse is inverse, because the inverse of 0 is defined as 0 and the inverse of 1 is also defined as 1 ok.

So, therefore you can actually ignore the inverse in the smaller field. And the with some simplifications, you can see that you will get d 0 and d 1 as shown here ok. So, you see that it is very simple in this field, because essentially you are just writing d 0 as g 1 and d 1 as g 0. So, basically the inverse in this field is actually kind of free, there is no computation that you need to do ok.

So, and that is also you know like you can also observe this that this also means that the squaring in this field will also be equal equally easy ok. So, the squaring and the inversion both in the normal basis. In the lowest field is actually free as unlike your polynomial basis, where you probably need some XOR gates ok. So, therefore right I mean so that that is an incentive for going to the normal basis ok.

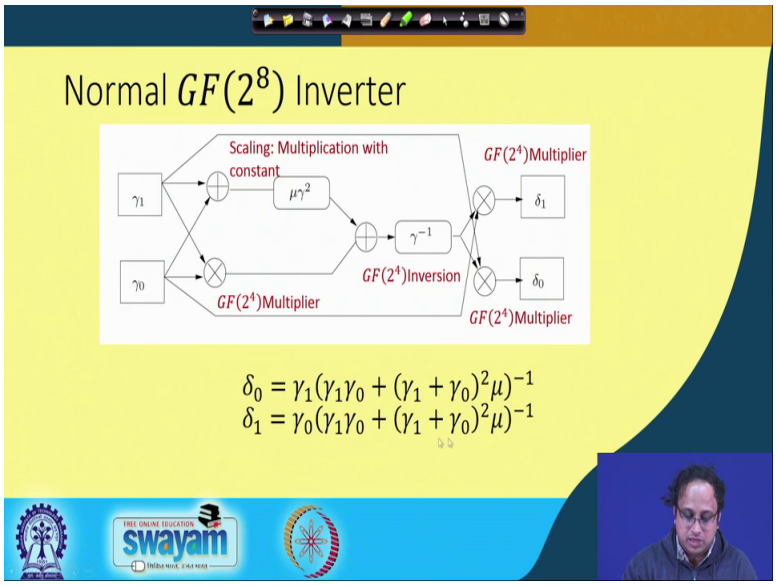
(Refer Slide Time: 21:01)




So, likewise what we can do is now, we can actually try to look for optimizations like what we have seen in the polynomial basis context ok. And you can note that the tau actually appears in both the equations, and therefore exactly like in the polynomial basis, we can set tau as 1 ok. Note that I cannot set mu equal to 1 for the reasons, which I told in the last class ok. Essentially right this essentially then would become a subfield of this particular field ok.

So, therefore right I will set tau as 1, but I will not set mu as 1 ok, but at least settling tau equal to 1 gives me a nice opportunity for optimization. For example, now this becomes in this form, and therefore you can write this as gamma 1 gamma 0 plus this whole square you can actually write as gamma 1 plus gamma 0 whole square ok, because you know that again when you are taking a square then 2 is 0, so therefore this is equivalent. Why do you do that you save some gates, because otherwise you have to do two squaring and then one addition, but now you have to just do one addition and one squaring ok.

(Refer Slide Time: 22:04)




And also you can write this in a nice or you can draw this in a nice way, for example here is my corresponding diagram for doing the normal GF 2 to the power of 8 inverter or you can say actually these are normal GF 2 power of 4 whole square inverter, because my element has we written in GF 2 power of 4 square.

So, therefore now when I have got two components like gamma 1 and gamma 0, you can see and you can exactly do a one to one match between this equation. So, you see that what I have got is gamma 1 into gamma 0, so this goes to my smaller inversion which is my GF 2 power of 4 inversion, which is denoted here. And the inputs to this is nothing but gamma 1 into gamma 0, gamma 1 into gamma 0 is done by this multiplier. And then I add it with gamma 1 plus gamma 0 whole square into mu ok.

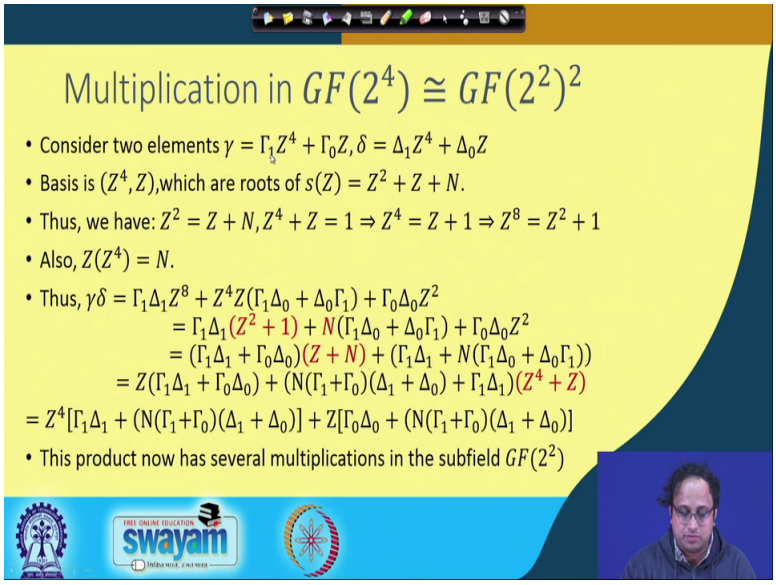
So, this operation so this operation is actually what is what we have seen previously and is called as the squaring and scaling operation ok. So, this operation where you are doing a squaring and your multiplying with a constant is called as a squaring and scaling operation ok. And that is done by this block, where you basically square and you scale that is you multiply with a constant ok. So, once you have done this, and you are doing this two I mean the input is the XOR of gamma 1 and gamma 0, and that is what you are squaring and scaling ok.

So, therefore once you have this part, and you have got gamma 1 into gamma 0, you basically XOR them to get your result, which you feet to this GF 2 power of 4 inversion.

And therefore, right you now get this part as you are output, and in one case you multiply with gamma 1. For example, for delta 0 you multiplied with gamma 1, so I take gamma 1 and I multiply here and I get delta 0. And likewise here I get gamma 0, and I multiply here to get delta 1 ok.

So, therefore right this quite easily understood from this diagram. And finally, right once you have done this right you can actually observe that internally you are basically doing GF 2 power of 4 inversions and GF 2 power of 4 multiplier. So, now you need to know the circuit for doing a GF 2 power of 4 multiply ok.

(Refer Slide Time: 24:19)




So, therefore right let us take a look into GF 2 power of 4 multiplied remember my elements in GF 2 power of 4 have been now are can be a isomorphically expressed in GF 2 power of 2 whole power of 2. And therefore, the elements here are gamma and delta ok. So, gamma as I told you is that nothing but gamma 1 Z to the power of 4 plus gamma 0 Z, because my basis Z power of 4 and Z. Likewise, delta is equal to delta 1 Z power of 4 plus delta 0 ok.

So, if I now multiply them ok, of course maybe you should note few more things that is the basis is Z power of 4 comma Z, which are the roots of this irreducible polynomial Z square plus Z plus N ok. And now what is this N? So, therefore right what I have is a Z power of Z so that means, like Z square is equal to Z plus N an exactly like what you

have done for GF 2 power of 4 square, we can do it for GF 2 power of 2 whole power of 2 also ok.

So, what is that we can write now that Z square plus Z is N, when I am do when I want to do my simplifications. And I can also write Z to the power of 4 plus Z is equal to 1 ok, because that is the sum of the two roots. And therefore, write Z Z to the power of 4 equal to Z plus 1, and that is Z power of 8 is equal to Z square plus 1 ok, I have just done squarings on both sides. Also the product of the two roots that is Z and Z power of 4 should be equal to this constant N ok.

So, therefore now I am ready to do this multiplication. So, if I do this multiplication, again I will have got terms like Z power of 8, because Z power of 4 and Z power of 4 will get multiplied. I will have terms like Z power of 4 into Z for with this will be my corresponding coefficient, and likewise I will have delta 0 into gamma 0 Z square ok.

So, now what I can do is I can replace this Z power of 8 as Z square plus 1. So, basically I just take this simplification that is Z power of 8 is equal to Z square plus 1 and I plug it over here. The product of this is written as N ok, and I get this part. So, likewise again I have to bring the result back into Z power of 4 and Z, which is my basis. And therefore, write I just do again a similar trick, which is I replace you know like Z; Z square as Z plus N and I get two parts that is one which as got essentially Z, and other part which is a constant.

But, now I replace this 1 by you know like because I have to I have to write 1 as Z power of 4 plus Z ok. So, therefore if I do that, then I just plug it over here. And finally, write so therefore I plug in this Z power of 4 plus Z ok. And if I do that means, I basically instead of one, I write this Z power of 4 plus Z ok. And the other term already has Z which is fine which is in my basis, Z is a basis element.

And therefore, right I split my result into two parts. One which has got Z, and the other which has got Z power of 4 ok. So, this product will again have now more multiplications in the subfield GF 2 power of 2 ok. So, therefore right this so what we have seen till now is that we have seen, how we can essentially get my get the result in GF 2 power of 2 power of 2 ok. So, basically we started with GF 2 power of 4 whole square, we did our multiplications in GF 2 power of 4. We saw how we can do

multiplications in GF 2 power of 4 by expressing there was elements in GF 2 power of 2 whole power of 2 ok.

So, now we are need a position to derive you know like the corresponding equations of the underlined fields? We basically have to consider one very important step, which is which I already tried to point out in the circuit diagram, which is the squaring and the scaling operation ok. And that is the crux operation, why are the crux of the operations, why the normal basis representation in so efficient in the so compact, and that we will study in the next class ok.

Thank you.