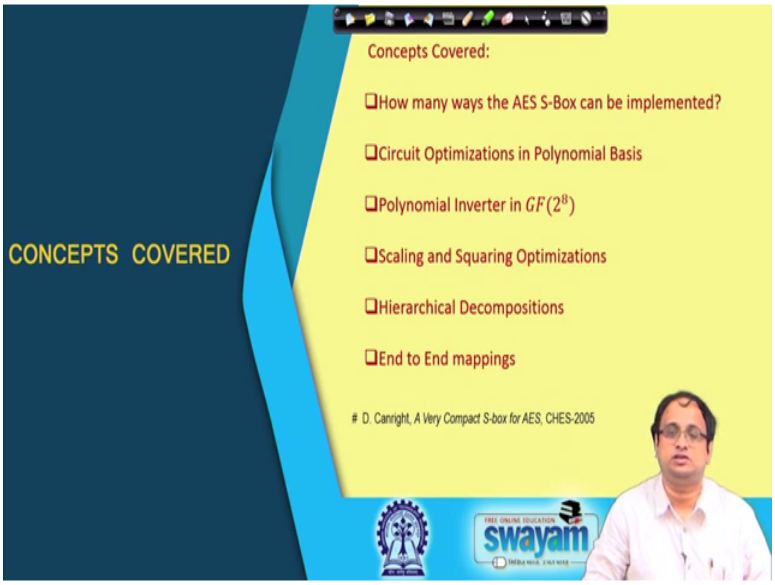
Hardware Security
Prof. Debdeep Mukhopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 15
Compact AES S – Box

So, welcome to this class on Hardware Security. Today, we shall be trying to look into specific block of a AES, which we have already being referring as the AES S-box or the sub bytes. So, we will we shall take a closer at the AES S-box and try to see a very interesting work about how you design compact AES S-box on hardware.

(Refer Slide Time: 00:37)



Concepts Covered:

❑How many ways the AES S-Box can be implemented?

❑Circuit Optimizations in Polynomial Basis

❑Polynomial Inverter in $GF(2^8)$

❑Scaling and Squaring Optimizations

❑Hierarchical Decompositions

❑End to End mappings

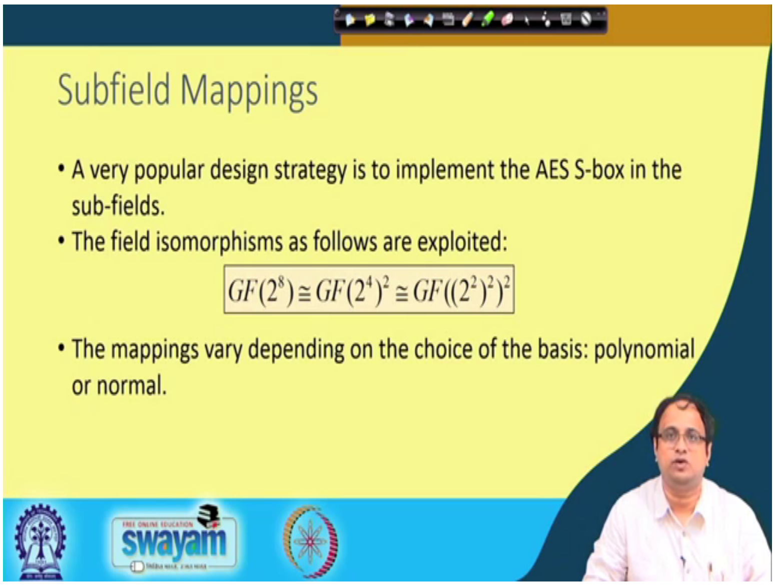
D. Canright, A Very Compact S-box for AES, CHES-2005

So, what we shall be trying to cover several topics in this in this part. So, we shall be trying to first of all understand in how many ways the AES S-box can be implemented. We shall be trying to look in specific about into the polynomial basis. We have discussed there are two types of basis like polynomial as well as normal basis. So, in particular we shall be trying to look into polynomial basis and try to see some circuit optimization techniques. We shall be looking into the in polynomial inversions circuit in GF 2 power of 8 and the I shall be taking about some important sub operations like one of them is scaling and squaring.

And we shall be discussing about how we can do optimization on it. And in particular right the main theme of this work could be how what is called as hierarchical decomposition or where essentially we decompose field in from in GF 2 power 8 to a sub field, which is GF 2 power of 4 square. And the again break up the GF 2 power of 4 into GF 2 power of 2.

So, we basically have a higher hierarchic hierarchical way of developing this design and that is what the we shall be trying to understand. And finally, we shall be concluding with a discussion on how do we can do an end-to-end transformation, because at the end of the day we need input and the output to remain the same as that in the original AES specifications. So, in particular this work will be you know like largely based on this work by D. Canright, which was published in CHES in 2005. And it is a very interesting work on a designing compact S-box for AES.

(Refer Slide Time: 02:09)



Subfield Mappings

- A very popular design strategy is to implement the AES S-box in the sub-fields.
- The field isomorphisms as follows are exploited:

$$\boxed{GF(2^8) \cong GF(2^4)^2 \cong GF((2^2)^2)^2}$$

- The mappings vary depending on the choice of the basis: polynomial or normal.

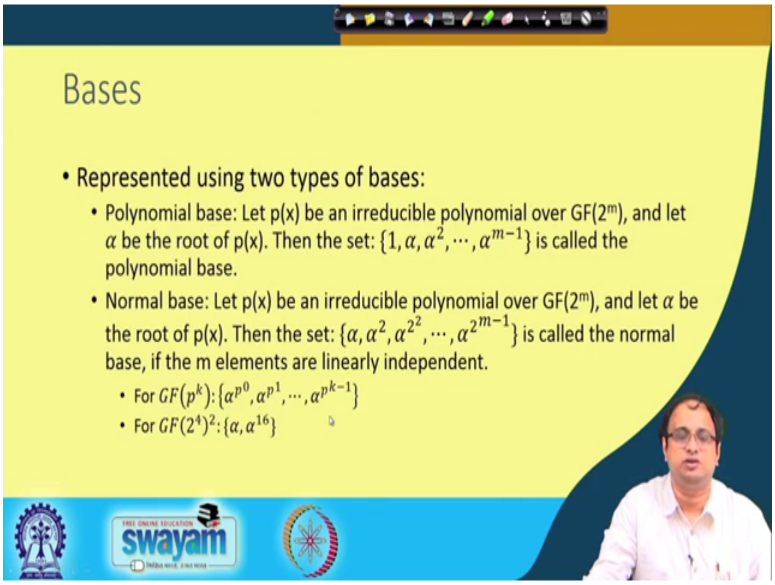
So, just to recapitulate, we are already have been discussing about this in our previous classes that we have already been discussing about field isomorphisms. So, the spirit of this work is based on field isomorphisms. So, the idea is that we have got the field GF 2 power of 8 as originally specified in the AES specifications.

We try to find out or express it eco equivalently in GF 2 power of 4 square and then again that is isomorphisms to GF 2 power 2 power of 2 power of 2. The idea is that if you want to do an operations say final field inverse GF 2 power of 8, then it is very costly. So, we try to therefore express that or convert that in to a field GF 2 power of 4 square by applying an isomorphic mapping ok, but the idea is that the underlying operations are now done in GF 2 power of 4 rather than GF 2 power of 8 ok.

So, therefore the cost in GF 2 power of 4 is significantly less compare to GF 2 power of 8. Likewise, we try to express GF 2 power of 4 in GF 2 power of 2 whole power of 2 ok and therefore, in the sub field GF 2 power of 2 the operations are now done. So, therefore you consider this right GF 2 power of 2 is only 2 bits of data. So, therefore the underlying operations becomes much more simple ok.

At the and also right since they are isomorphic, you can actually transform this field into GF 2 power of 2 power of 2. And you can do your operations in this field in an more efficient manner. And then again you can apply the reverse mapping to get back to the GF 2 power of 8. Remember that our AES operates in GF 2 power of 8. So, we should be avail to operate get the result back in the original field in the original target field. So, there are different types of mappings, we can define and different types of implementations can also emerge because of them. And they often are guided by the choice of the underlying basis like polynomial basis or normal basis ok.

(Refer Slide Time: 04:03)



Bases

- Represented using two types of bases:
  - Polynomial base: Let p(x) be an irreducible polynomial over GF(2^m), and let α be the root of p(x). Then the set: $\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$ is called the polynomial base.
  - Normal base: Let p(x) be an irreducible polynomial over GF(2^m), and let α be the root of p(x). Then the set: $\{\alpha, \alpha^2, \alpha^{2^2}, \cdots, \alpha^{2^{m-1}}\}$ is called the normal base, if the m elements are linearly independent.
    - For $GF(p^k)$: $\{\alpha^{p^0}, \alpha^{p^1}, \cdots, \alpha^{p^{k-1}}\}$
    - For $GF(2^4)^2$: $\{\alpha, \alpha^{16}\}$

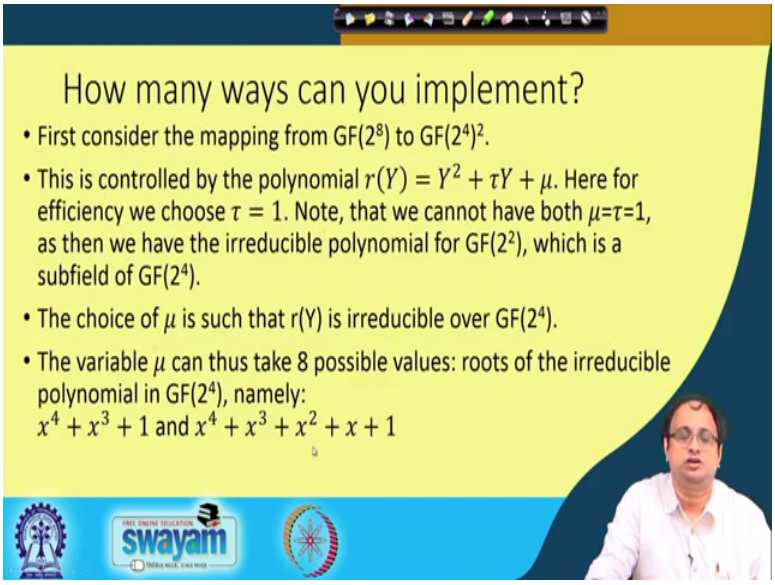
So, we are already discussed about thus that here is a quick recap on that. So, there are two types of bases ok. So, one is called as a polynomial base and other one is called as an normal base. So, if you take as you know like for every extension field like GF 2 power of m that is an irreducible polynomial as we have discussed, p x whose degree is m if the field is GF 2 power of m and let alpha be the root of p x ok. So, if alpha is a root of the p of of p x, then the set one alpha alpha square so on till alpha to the power of m minus 1 is called the polynomial base ok. So, there are m elements in this base ok. So, therefore we can express any field element as an linear combination of these bases elements ok.

Likewise, there is also another bases which is called as the normal bases. So, in normal bases again you have p x which is an irreducible polynomial over GF 2 power of m, and let alpha be the root of p x ok. So, then your set alpha power alpha, alpha square, again alpha to the power of 2 power of 2, so these are all powers of 2 of alpha ok. Likewise, you again do m such our m such powers of 2 that means, the final result is alpha to the power of 2 to the power of m minus 1 ok so, these are called as a normal bases, if the n elements are linearly independent ok.

So, example like for example GF p power of k, you can actually in generalize it to say GF p power of k or also. In that case the normal bases elements will be alpha to the power of p power of 0, alpha to the power of p power of 2, so until alpha to the power of p power of k minus 1. So, again there are k since this is k, there are k elements is the normal bases.

As a special example which we will be using in our work. For example, consider GF 2 power of 4 square ok. In GF 2 power of 4 square, there are two bases elements ok; one is alpha, the other one is alpha to the power of 60 ok, so that is the essentially you know like the normal bases of GF 2 power of 4 square ok. Likewise, we will have we will have being normal bases for GF 2 power of 2 ok and essentially that will be alpha and alpha to the power of 4 ok. So, we can essentially enumerate the normal bases elements using this idea ok.

(Refer Slide Time: 06:23)



How many ways can you implement?

- First consider the mapping from $GF(2^8)$ to $GF(2^4)^2$.
- This is controlled by the polynomial $r(Y) = Y^2 + \tau Y + \mu$. Here for efficiency we choose $\tau = 1$. Note, that we cannot have both μ=τ=1, as then we have the irreducible polynomial for $GF(2^2)$, which is a subfield of $GF(2^4)$.
- The choice of μ is such that r(Y) is irreducible over $GF(2^4)$.
- The variable μ can thus take 8 possible values: roots of the irreducible polynomial in $GF(2^4)$, namely: $x^4 + x^3 + 1$ and $x^4 + x^3 + x^2 + x + 1$

So, therefore right first so let us try to effort first of all kind address or answer to these question. How many ways can you implement the mapping mean the AES S-box ok? So, by using this concept of what is called as the hierarchical decomposition or it is often also called as tower fields ok. So, first consider the mapping from GF 2 power of 8 to GF 2 power of 4 square ok. So, this is controlled by the polynomial r Y, which is essentially nothing but Y square plus tau Y plus mu ok. So, this is an irreducible polynomial in GF 2 power of 4 square ok.

So, now you know like for we as we will discussing right for efficiency we choose this tau equal to 1, because you will see this tau appears in many output equations, therefore to make it you know like efficient we will we will be we can actually plugin tau equal to 1 can be fixed tau is equal to 1.

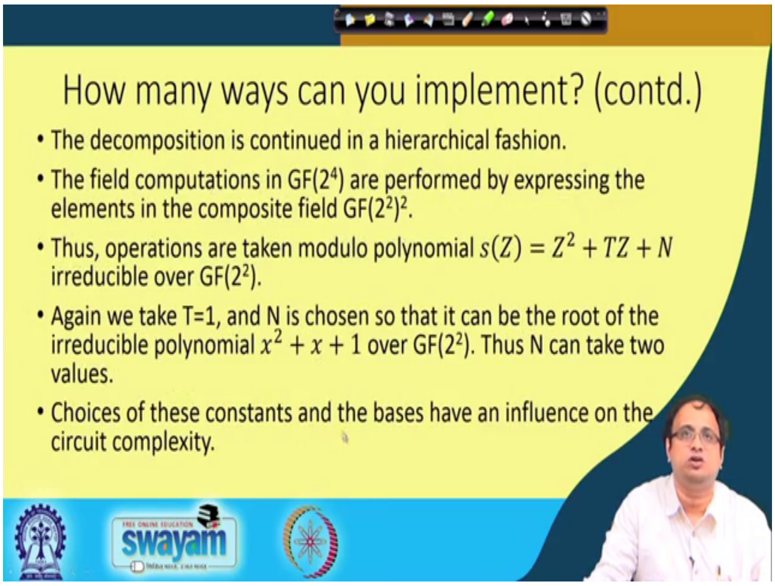
So, note that we cannot make both mu and tau 1. Because, if you make both tau and tau and mu 1, then this turns out to be Y square plus Y plus 1 ok, and that is a actually an irreducible polynomial for GF 2 power of 2 ok. So, Y squared plus Y plus 1 is an irreducible polynomial for GF 2 power of 2, which is actually sub field of GF 2 power of 4 ok. But, what we want is that we want that the choice of mu should be such that r Y that is Y square plus tau Y plus mu. So, if you plug tau equal to 1, Y square plus Y plus mu is irreducible over GF 2 power of 4 ok.

And if you want to make Y square plus Y plus mu irreducible over GF 2 power of 4, then an then mu needs to satisfy or mu is essentially a root of the irreducible polynomial in GF 2 power of 4 ok, so that means right if you express mu as a polynomial in, then you know it does not factor in the field GF 2 power of 4 ok.

So, there are two irreducible polynomials right. So, therefore mu can take 8 possible values so mu can take 8 possible values, you can see that you know like the 4 the 4 roots will come from this equation x power of 4 plus x power of 3 plus 1, which is an irreducible polynomial of GF 2 power of 4.

You can get distinct 4 roots, if you solve the penta pentanomial x to the power 4 plus x to the power of t3 plus x square plus x plus 1, which is also another irreducible polynomial of a different kind for GF 2 power of 4 ok. So, therefore this equation or this polynomial give 4 roots, this polynomial will give 4 roots. And therefore, in total you have got 8 possible values of mu, you can have 8 possible choices for mu ok. But, note that we have fixed tau as 1 in our discuss in our implementations.

(Refer Slide Time: 09:19)



How many ways can you implement? (contd.)

- The decomposition is continued in a hierarchical fashion.
- The field computations in GF(2^4) are performed by expressing the elements in the composite field GF(2^2)^2.
- Thus, operations are taken modulo polynomial $s(Z) = Z^2 + TZ + N$ irreducible over GF(2^2).
- Again we take T=1, and N is chosen so that it can be the root of the irreducible polynomial $x^2 + x + 1$ over GF(2^2). Thus N can take two values.
- Choices of these constants and the bases have an influence on the circuit complexity.

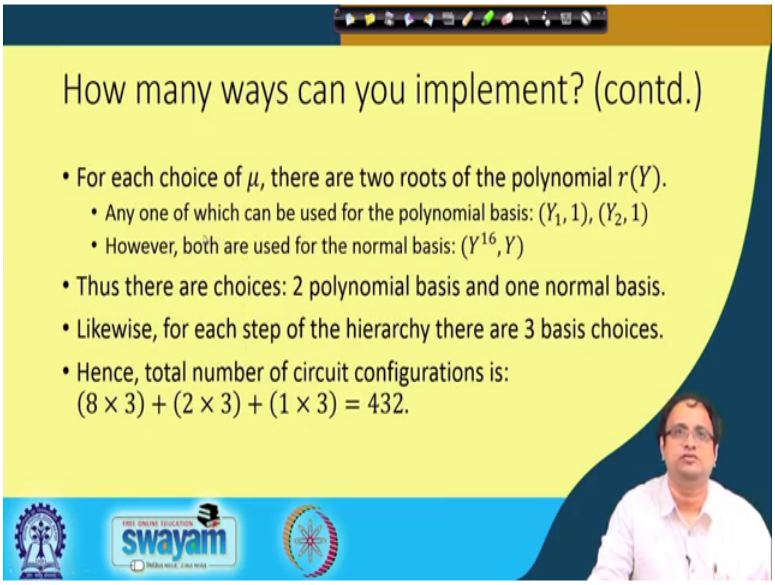
So, likewise you can you know you can actually continue your decomposition in an hierarchical fashion. The field computations in GF 2 power of 4 are performed by expressing the elements. Now, in the composite field GF 2 power of 2 ok.

So, again this is control by the modulo of polynomial by taking modulo of the with the irreducible polynomial s Z where s Z is now Z square plus T Z plus N ok. Note that I have used you know like Y to denote the tough field Y means, the I have use the indeterminate Y to denote the tough field that is GF 2 power of 4 square. And I have use the indeterminate Z to denote the field GF 2 power of 2 power of 2 GF 2 power of 2 whole power of 2 ok.

So, therefore here again write this is an irreducible polynomial over GF 2 power of 2. So, again you know like we make T equal to 1 like previous case. Like when we had previously we made tau 1, now we make T 1 and N chosen, so that so this capital N is chosen, so that it can be the root of the irreducible polynomial x square plus x plus 1 over GF 2 power of 2 ok. So, therefore write this equation as got two roots and therefore N can take two possible values ok.

So, now we have kind of enumerated how many values mu can take and how many values N can take. In order to understand, how many such circuits we can realize with them ok. So, the circuit complexity will be decided by these constants that is mu and N as well as the underlying bases of your implementation, whether you are choosing polynomial bases or whether you are using normal bases ok.

(Refer Slide Time: 11:07)



How many ways can you implement? (contd.)

- For each choice of μ, there are two roots of the polynomial $r(Y)$.
  - Any one of which can be used for the polynomial basis: $(Y_1, 1)$, $(Y_2, 1)$
  - However, both are used for the normal basis: (Y^{16}, Y)
- Thus there are choices: 2 polynomial basis and one normal basis.
- Likewise, for each step of the hierarchy there are 3 basis choices.
- Hence, total number of circuit configurations is: $(8 \times 3) + (2 \times 3) + (1 \times 3) = 432.$

So, for example right if you are using polynomial bases for each choice of mu that is suppose I fix mu, then your polynomial r Y gets fixed right, because your r Y is Y square plus tau Y plus mu, so tau is 1. If I fix mu, then this polynomial gets fixed. And therefore, write of this equation that is Y square plus Y plus mu, we left two roots ok.

Each of this roots can be independently used as the polynomial bases. So, I can choose either the polynomial bases as Y 1 comma 1 or I can choose the polynomial the bases as Y 2 comma 1, both of them are polynomial bases. But, if I want the nominal basis, then there are two roots again ok. And as we have discussed the roots will be Y and Y power of 16, because this field is GF 2 power of 4 square, so this is my normal basis. And both the roots will give me one normal basis ok. So, in total we will have three such basis representations ok.

So, again you know like thus there are two choices, two polynomial basis and one normal basis. Likewise, for each step of the hierarchy that means when you are going for GF 2 power of 8 to GF 2 power of 4 square and likewise from GF 2 power of 4 to GF 2 power of 2, you essentially have got three basis choices ok.

So, therefore now if we total the count total number of circuit configurations that we are trying to explore here is 8 multiplied by 3 ok that is your the you know like the tough field that is 8 power of 3 that is 24 ok and this is 2 into 3 which is 6 that is the that is because there are eight choices of mu and there are three choice of basis. So, it is 24 total possible ways.

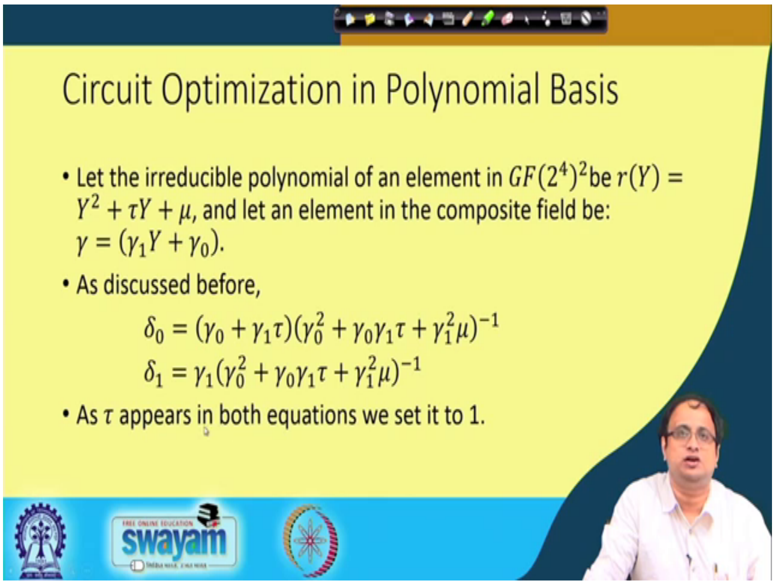
Likewise for GF 2 power of 2, you have got two choices for N and we have got three basis choices, so there are six of choices. For the smaller mode field like the smaller field there is no I mean there is no variation, so you just have got one, but you again can have three basis choices.

So, this is for when we are represent representing GF 2 power of 2 in terms of GF 2 ok. So, we have got three such transformation, which we are doing. Like GF 2 power of 8, you are writing as GF 2 power of 4 whole square. GF 2 power of 4 you are breaking as GF 2 power of 2 and GF 2 power of 2, you are breaking up as GF 2 whole power of 2, so you are writing it in terms of GF 2 ok.

So, the so again I am repeating this you are writing GF 2 power of 8 in terms of GF 2 power of 4, you are so here there are this is the case which is governing that. Likewise, you are expressing GF 2 power of 4 in terms of GF 2 GF 2 power of 2 that is this case ok and likewise you are writing GF 2 power of 2 in terms of GF 2 and that is case ok.

So, totally you write the number of cases this actually should be a product ok, so please replace this by a product. This as multiplication of 8 into 3 into 2 into 3 into 1 into 3 and this totally counts to 432 ok. So, there are totally 432 possible ways in which we can have circuits. And you can have what we want to kind of explore is this I would say design space ok and we want to see that where are the opportunities of optimization ok.

(Refer Slide Time: 14:31)



Circuit Optimization in Polynomial Basis

- Let the irreducible polynomial of an element in $GF(2^4)^2$ be $r(Y) = Y^2 + \tau Y + \mu$, and let an element in the composite field be: $\gamma = (\gamma_1 Y + \gamma_0)$.
- As discussed before,

$$\delta_0 = (\gamma_0 + \gamma_1\tau)(\gamma_0^2 + \gamma_0\gamma_1\tau + \gamma_1^2\mu)^{-1}$$
$$\delta_1 = \gamma_1(\gamma_0^2 + \gamma_0\gamma_1\tau + \gamma_1^2\mu)^{-1}$$

- As τ appears in both equations we set it to 1.

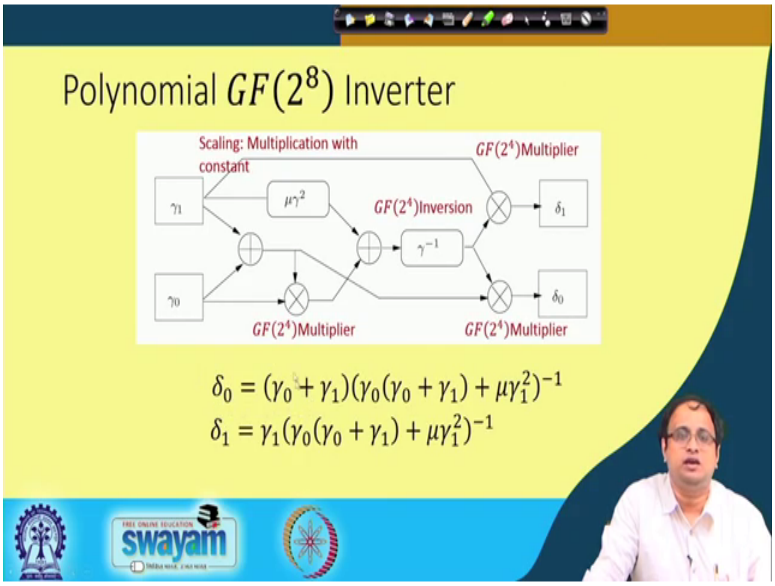
So, basically right I mean so let us try to look it in look them look in to the in the one by one. So, first of all let the irreducible polynomial of an element. So, remember that now we are considering this we are considering that GF 2 power of 8 or element in GF in 2 power of 8 has been transformed to an element in GF 2 power of 4 square ok.

So, there my polynomial is r Y, which is Y square plus tau Y plus mu ok and let an element in the composite field therefore so in the so therefore it will look like this gamma 1. So, gamma is an element in this field and I can write it as gamma 1 Y plus gamma 0 ok. So, this is my polynomial basis way of writing it, I am writing this using the polynomial basis ok.

So, Y is essentially the root of this equation and I choose one such value of Y. And therefore, I can express gamma as gamma 1 Y plus gamma 0 ok. So, this is what we have already discussed in one of our previous classes, how we can write the inverse of gamma say gamma 1 plus gamma 0's inverse is delta 1 Y plus delta 0. And therefore, write delta 1 and delta 0 can be enumerated in this way ok. So, this is something that we have already discussed in one of our previous classes.

So, I am not repeating that derivation. But, I am trying to stress here that tau for example appears in both the equations ok and that is essentially what is motivating us to say tau as 1. So, as both the equations gets simplified ok. As tau appears in both the equations, we set it to 1 ok.

(Refer Slide Time: 15:59)



Polynomial $GF(2^8)$ Inverter

$$\delta_0 = (\gamma_0 + \gamma_1)(\gamma_0(\gamma_0 + \gamma_1) + \mu\gamma_1^2)^{-1}$$
$$\delta_1 = \gamma_1(\gamma_0(\gamma_0 + \gamma_1) + \mu\gamma_1^2)^{-1}$$

So, now if you do that, then you can do some more simplifications. For example, you can write this for example if you observe this term, which is gamma 0 square plus gamma 0 gamma 1 plus gamma 1 squared mu. Note that now I can take gamma 0 common from here. And therefore, I can write this as gamma 0 into gamma 0 plus gamma 1 plus mu gamma 1 square ok.

So, this is again I am taking an inverse. Note that this element is now in GF 2 power of 4 ok, likewise all this multiplications are now in GF 2 power of 4 ok. So, if you want to describe this in the form of a circuit this how it will look like. So, I have got my inputs gamma 1 and gamma 0. Gamma 1 is the higher nibble, gamma 0 is the lower nibble. And if I want to say calculate the output delta 1 and delta 1, so then I can just trying to understand the relation of this circuit with this equations ok.

So, first of all let us start with delta 1. So, delta 1 is nothing but we are computing an inverse of the part which is inside the first parenthesis. So, if you observe here, we take an XOR of gamma 1 and gamma 0. So, this is essentially computing this part gamma 1 plus gamma 0 and then you are multiplying this with gamma 0. So, note that this XOR is in GF 2 power of 4, this multiplication is also in GF 2 power of 4. So, this is where we using GF 2 power of 4 multiply.

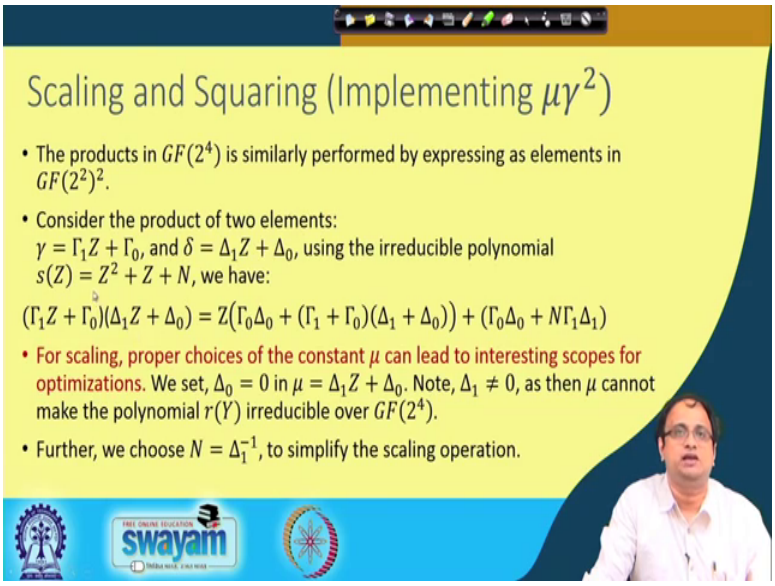
So, then we are adding this with an output which is mu gamma 1 square ok. So, this part that is mu gamma 1 square is where I am feeding one input, if the input is gamma 1. And this is computing mu gamma square which is if I feed in gamma 1 as input, the output will be mu gamma 1 square ok. So, this mu gamma 1 square is now added with this part, so therefore gamma 0 into gamma 0 plus gamma 1. And then the total part right the total essentially this output is fade GF 2 power of 4 inversion circuit.

So, therefore I get this inversion and this inversion is now multiplied with or has to be multiplied with a component. So, therefore this right is essentially if you observe if you observed the delta 1 circuit, then I am multiplying this with gamma 1 ok. So, therefore if I multiply gamma 1, I get this part which is delta 1. And if I multiply gamma 0 plus gamma 1 that means, I just take this part out and again I multiply with the GF 2 power of 4 multiply with the output of this inversion circuit, then I get delta 0 ok.

So, this pretty much explains the circuit and shows how it corresponds with this equations ok. And note that this operation is something that we will be trying to stress in our talk that is what we call as scaling. So, this so the idea is that this mu is a constant, and therefore write when you are try to implement and circuit where do you are multiplying a constant you do not apply a full floor multiplier, because that will lead to wastage of gates. Rather you optimize your circuit and we call that special circuit which multipliers multiplies with a constant as a scaling circuit ok.

In particular here, we are actually do a squaring and then scaling ok. And therefore, this circuit is what we will be calling as scaling and squaring ok. So, therefore we will first square and then scale. And we will see that why we do that this there is a lot of opportunity of optimization, when you considered this circuit ok.

(Refer Slide Time: 19:23)



Scaling and Squaring (Implementing $\mu\gamma^2$)

- The products in $GF(2^4)$ is similarly performed by expressing as elements in $GF(2^2)^2$.
- Consider the product of two elements: $\gamma = \Gamma_1 Z + \Gamma_0$, and $\delta = \Delta_1 Z + \Delta_0$, using the irreducible polynomial $s(Z) = Z^2 + Z + N$, we have:

$$(\Gamma_1 Z + \Gamma_0)(\Delta_1 Z + \Delta_0) = Z\big(\Gamma_0\Delta_0 + (\Gamma_1 + \Gamma_0)(\Delta_1 + \Delta_0)\big) + (\Gamma_0\Delta_0 + N\Gamma_1\Delta_1)$$

- For scaling, proper choices of the constant μ can lead to interesting scopes for optimizations. We set, $\Delta_0 = 0$ in $\mu = \Delta_1 Z + \Delta_0$. Note, $\Delta_1 \neq 0$, as then μ cannot make the polynomial $r(Y)$ irreducible over $GF(2^4)$.
- Further, we choose $N = \Delta_1^{-1}$, to simplify the scaling operation.

So, now what we want to observe is that therefore this brings us to this scaling and squaring operation. And we want to essentially do a scaling and squaring that means, we want implement this step mu into gamma square ok. And we want to see how we can efficiently implement this. So, the product in GF 2 power of 4 is similarly performed by expressing an elements in GF 2 power of 2. So, therefore, now we are considering the products in GF 2 power of 4. So, if you observe the circuit here, these operations are in GF 2 power of 4.

So, now I am expressing or we are trying to kind of hierarchically go into this circuit and imagine that this GF 2 power of 4 is now written recursively in terms of GF 2 power of 2 ok. So, therefore right this is the 4 bit operation, GF 2 power of 2 will again have two parts, each of them having two bits ok. So, totally it will have four parts.

So, now, therefore, you can actually express the product in GF 2 power of 4 in a similar way as element in GF 2 power of 2 whole power of 2 and the for that right consider the product of two elements. So, again now we will be using Z as I have discussed here. So, Z is my inter indeterminant in this field. And therefore, one elements are say gamma and delta which I want to implement which I want to multiply.

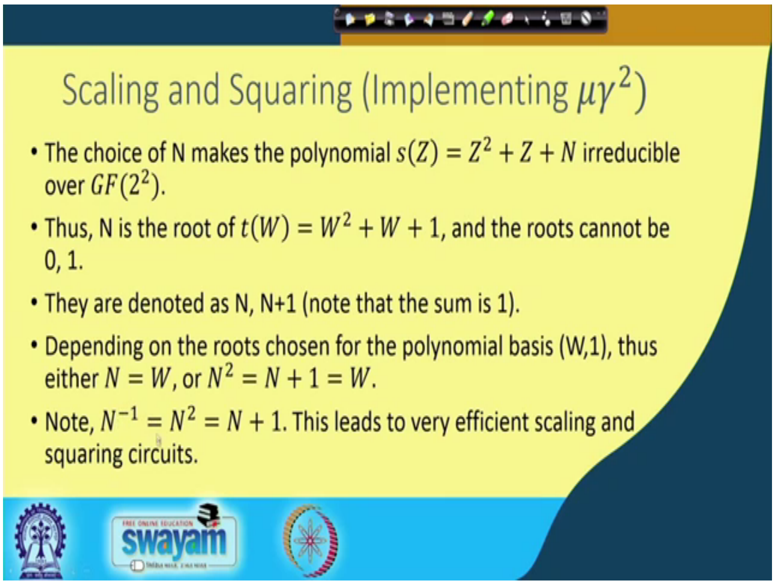
So, gamma is an element in GF 2 power of 2 whole power of 2. And it when I express gamma as capital gamma 1 Z plus capital gamma 0, then gamma 0 or capital gamma 0 and capital gamma 1 are both elements of GF 2 power of 2 ok. Likewise your delta which is another element in GF to power of 2 whole power of 2 ok, we can also be written as capital delta 1 Z plus capital delta 0 and each of this delta capital delta 0 and capital delta 1 belong to the sub field which is GF 2 power of 2.

So, now when I multiplying these two elements, I have to use an irreducible polynomial as usual. And the irreducible polynomial in this case is s Z which is nothing but Z square plus Z plus capital N. So, when I am multiplying these two things, we can observe that there will be kind of term will I will get a Z squared ok. And therefore, this simplification is a result of the fact that I have replaced Z square with Z plus N ok. So, therefore, the moment I replaced Z squared with Z plus N, you can actually verify it you should be able to get this equation. So, therefore, I replace Z square as Z plus N and the essentially this should follow.

So, now, if when I am try to do a scaling right, scaling is nothing but a multiplication, but only that of the fact is one of the multiplication input or one of the multiplication argument is a constant ok. So, in this case my say you know like for example, your input is gamma 1 Z plus gamma 0, but you are to trying to scale with this input that is delta 1 Z plus delta 0 ok. So, therefore, this mu right essentially this is nothing but mu and mu we can actually control ok.

So, for example, right as I have said that I can set delta 1 you know like I will got two inputs two components here delta 1 and delta 0. Suppose, I make delta 0 as 0, that means, I said delta 0 equal to 0. Note that I cannot make delta 1 as 0, because if I do delta 1 as 0, then you cannot make the polynomial r Y irreducible over GF 2 power of 4. So, therefore, I will have some restriction. And with that restriction I can make mu is equal to delta 1 Z ok. And we will further choose we was as we will see later on that delta 1, we will we will make it as N inverse or the inverse of N. And we will make N as delta 1 inverse to simplify the scaling operation ok. For just keep in mind that mu is nothing but delta 1 Z that means I have said delta 0 to 0 ok.

(Refer Slide Time: 23:15)



Scaling and Squaring (Implementing $\mu\gamma^2$)

- The choice of N makes the polynomial $s(Z) = Z^2 + Z + N$ irreducible over $GF(2^2)$.
- Thus, N is the root of $t(W) = W^2 + W + 1$, and the roots cannot be 0, 1.
- They are denoted as N, N+1 (note that the sum is 1).
- Depending on the roots chosen for the polynomial basis (W,1), thus either $N = W$, or $N^2 = N + 1 = W$.
- Note, $N^{-1} = N^2 = N + 1$. This leads to very efficient scaling and squaring circuits.

So, with this inputs when I am trying to do scaling and squaring operation, so the choice of N right, so therefore, you can observe that the choice of N when you are trying you know like essentially as we have said that the choice of N also cannot be arbitrary. If the choice of N is has to be such that it makes this polynomial s Z, which is equal to Z square plus Z plus capital N irreducible over GF 2 power of 2 ok. So, note that there for that purpose N has to be a root of the polynomial t W, which is again we have when you are expressing GF 2 power of 2 in terms of GF 2 whole power of 2 ok, that means, you are expressing it as elements of GF 2 now ok.

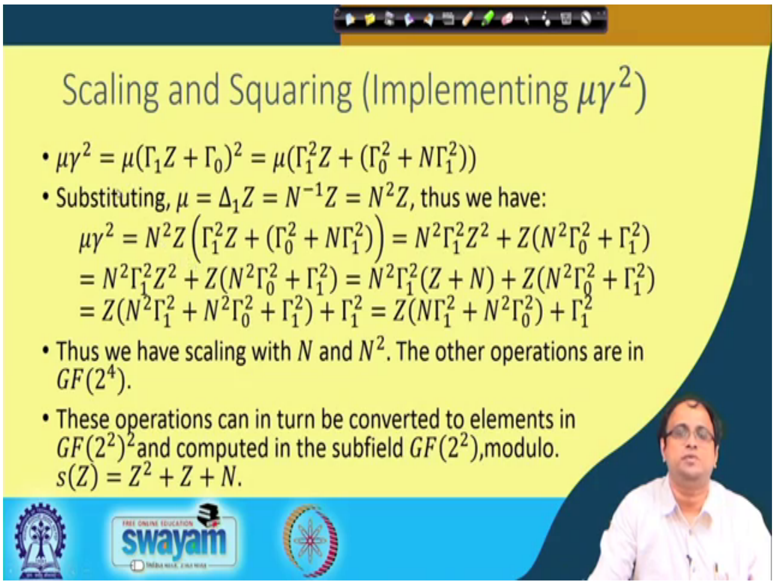
So, then the corresponding polynomial is t W, which is omega square plus omega plus 1 ok. And the and you can easily observe that the roots cannot be 0 here, because if I plug in 0, I get 1 if I plug in 1, I also get 1. So, therefore, 0 and 1 cannot be roots of this equation, rather let me denote the roots as N and N plus 1. Note that the sum of the roots right of this equation has to be 1, but from the theory of equations ok. And the let us just symbolically denote one of the roots to be N and therefore, the correspondent correspondingly the other root is N plus 1.

So, depending upon the roots therefore, the polynomial, so depending upon the roots the chosen for the polynomial basis W comma 1 that means, you essentially for the lower field, you have got the basis as W comma 1 ok. And the therefore, write either N will be equal to omega or N will be equal to W or N square will be equal to W ok. So, you essentially have got two polynomial basis choices. You can either make N as omega W or you can make N square as W ok. Note that N square will be equal to N plus 1, because you know like N square plus N plus 1 will be equal to 0 ok.

And note that when you are talking about you know like this circuits right, then N to the power of minus 1 is equal to N square ok, so that is equal to N plus 1 that is N to the power of minus 1 is equal to N square which is equal to N plus 1 ok. So, these are small you know like important observations which we will be using in our optimizations in the you know like in the following discussion.

So, these optima or these small tricks right will lead to a very efficiency scaling and squaring circuits. So, therefore, these are something that we need to keep in perspective. So, note that you can easily verify these things for example, what you can do is that you can verify these results quite easily ok. If you can understand the does the field structure that we have been discussed.

(Refer Slide Time: 26:13)



Scaling and Squaring (Implementing $\mu\gamma^2$)

- $\mu\gamma^2 = \mu(\Gamma_1 Z + \Gamma_0)^2 = \mu(\Gamma_1^2 Z + (\Gamma_0^2 + N\Gamma_1^2))$
- Substituting, $\mu = \Delta_1 Z = N^{-1} Z = N^2 Z$, thus we have:

$$\mu\gamma^2 = N^2 Z\left(\Gamma_1^2 Z + (\Gamma_0^2 + N\Gamma_1^2)\right) = N^2\Gamma_1^2 Z^2 + Z(N^2\Gamma_0^2 + \Gamma_1^2)$$
$$= N^2\Gamma_1^2 Z^2 + Z(N^2\Gamma_0^2 + \Gamma_1^2) = N^2\Gamma_1^2(Z + N) + Z(N^2\Gamma_0^2 + \Gamma_1^2)$$
$$= Z(N^2\Gamma_1^2 + N^2\Gamma_0^2 + \Gamma_1^2) + \Gamma_1^2 = Z(N\Gamma_1^2 + N^2\Gamma_0^2) + \Gamma_1^2$$

- Thus we have scaling with N and N^2. The other operations are in $GF(2^4)$.
- These operations can in turn be converted to elements in $GF(2^2)^2$and computed in the subfield $GF(2^2)$,modulo. $s(Z) = Z^2 + Z + N$.

So, now with this background let us say you know like just let us try to understand this scaling and squaring circuit. So, for example, like when I am try to do mu gamma square, so mu gamma square is nothing but mu multiplied with gamma square. So, what is gamma, gamma is capital gamma 1 Z plus gamma 0 and I am doing a whole square on that so that is equal to mu into gamma 1 Z plus gamma 0 whole square and that essentially you can write as gamma 1 square. Again you can write it as Z square plus gamma 0 square, but note that you can replace Z square as Z plus N and therefore, with that simplification you will get this as your result ok.

So, now if I substitute mu as delta 1 Z, remember delta 0 I mean delta 1 cannot be 0. So, mu is delta 1 Z and I said that I have plugged in delta 1 as N to the power of minus 1, and I can also write N to the power of minus 1 as N squared Z ok. And if I do that, then mu gamma square or essentially this results in. So, if I plug in instead of mu I write N square Z, so I got N square Z multiplied with gamma 1 square Z plus gamma 0 square plus N gamma 1 square ok. And this turns out to be N square. So, I just take N square and I do an operation here.

So, N square multiplied with gamma 1 square and note that Z into Z I will get Z square plus Z, that means, Z comes here and then I multiply N square with this part that is N square into gamma 0 square plus N square into N that means N cube now N cube becomes 1 ok. So, therefore, I just get gamma 1 square ok. So, therefore, this essentially is equal to writing as N square gamma 1 square Z square which is the first.

So, now, let me just conclude this part by discussing about the final effect of these optimizations on scaling and squaring ok. So, therefore, scaling and squaring is nothing but calculating mu into gamma square. Remember that gamma is now denoted as gamma 1 Z plus gamma 0 and then I am doing a whole square on that. So, if I do that I will get gamma 1 square Z square plus gamma 0 square, remember that I am doing in characteristic two and then we will replace Z square with Z plus N ok.

So, therefore, if you do that you will get this as your result and remember that mu which is with which you are doing the scaling is a constant and that is essentially nothing but delta 1 Z ok. Remember delta 1 cannot be 0 so, it is some delta 1 delta 1 Z. And this delta 1 is say N to the power of minus 1 as we have taken as choice ok. So, N to the power of minus 1 is again equal to N square, because N to the power of 3 is 1 ok. You can easily understand this because N is an element in GF 2 power of 2 ok. If you do that write, then there four elements and therefore, write you can verify from formats little theorem that you will get N to the power of 3 as 1 ok.

So, therefore, write we can actually write N to the power of minus 1 Z as N square Z ok, and therefore, write it turns out that mu gamma square is nothing but I am writing N square Z multiply it with gamma square which is gamma 1 square Z plus gamma 0 square plus N gamma 1 square. So, now, if I apply N square over this part in the parenthesis, I will get N square gamma 1 square Z square plus Z multiplied with N square gamma 0 square which where I am multiplying this over this and then I have got N to the power of 2 into N which is N cube. Note that N cube is 1, so I get gamma 1 square.

So, this you can again write as N square gamma 1 square Z square plus Z into N square gamma 0 square plus gamma 1 square, this just copying this result. So, this is equal to N square gamma 1 square and now I can write Z square as Z plus N. So, replace Z square with Z plus N because I am doing a modulo with Z square plus Z plus N plus Z into N gamma N square gamma 0 square plus gamma 1 square. So, therefore, now if I just take the coefficients of Z and the constant part, then I will have Z into N gamma 1 squared plus N square gamma 0 square plus gamma 1 square ok.

So, note that you can easily verify that I have got N square is easy to verify that we have got N square gamma 0 square which comes here. But the other term that means, if I take gamma 1 square I will get N square plus 1 ok. And N square plus 1 is nothing but N, because N square plus N plus 1 is equal to 0 ok. So, therefore right this is your corresponding operation when you have done scaling and squaring, this is your final result here which is the result in this point. So, now, if you observe right, you can see that we have got scaling there are some intermediate scalings which we are doing.

In order to realize this scaling hierarchically you are doing other few you are do few more scaling. For example, here you are doing a scaling with N because your multiplying with N ok. And likewise here you are doing a scaling with N square ok. And the other operation is of course, you are doing an addition. So, you are also doing an addition here which you are doing ok. So, these operations are now essentially also needs to be tackled and needs to be again implemented. So, these operations can in turn be therefore, converted to elements in GF 2 power of 2 whole power of 2 and again computed in the sub field GF 2 power of 2 ok.

So, these operations are in GF 2 power of 4 because you have now successfully decomposed a GF 2 power of 8 operation into GF 2 power of 4. So, therefore, these operations that is the scaling the addition, all of them takes place in GF 2 power of 4. But you can also equivalently write GF 2 power of 4 isomorphically in this field GF 2 power of 2 whole power of 2 ok. And therefore, write you can compute in the subfield now GF 2 power of 2 modulo again s Z which is equal to Z square plus Z plus N ok.

So, therefore right this is something that we need to essentially again take a look at and we need to kind of continue about how we can you know like or what is the impact of or of this optimizations on this overall circuit ok and that is will what we will take up in the next class ok.

Thank you.