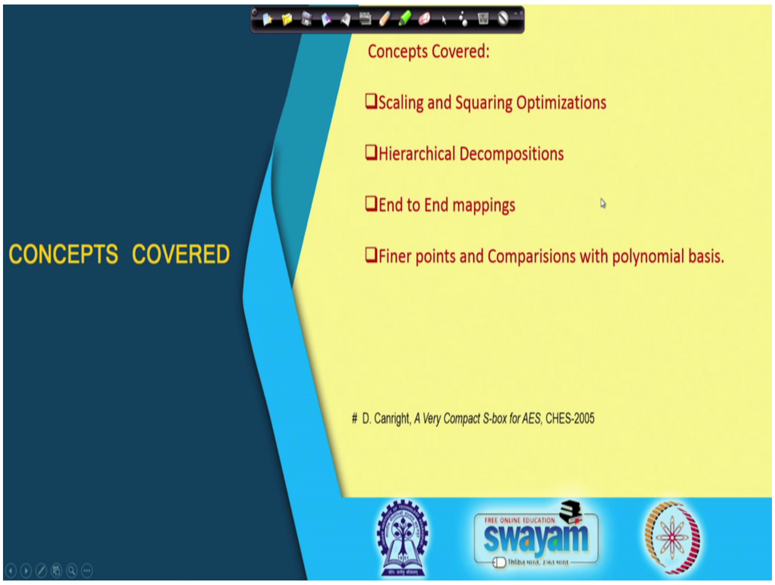
Hardware Security
Prof. Debdeep Mukhopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 18
Compact AES S – Box in Normal Basis (Contd.)

Welcome back to this class on Hardware Security. So, we shall be continuing our discussion on finding out the Compact AES S Box for Normal Basis representation.

(Refer Slide Time: 00:27)



CONCEPTS COVERED

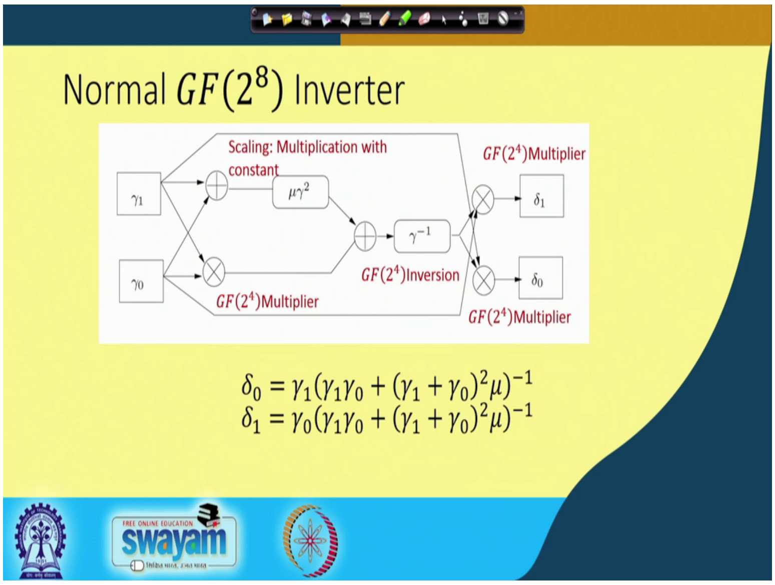
Concepts Covered:

- ❑Scaling and Squaring Optimizations
- ❑Hierarchical Decompositions
- ❑End to End mappings
- ❑Finer points and Comparisions with polynomial basis.

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

So, if you remember in the last class we essentially stopped at the scaling and squaring optimizations, and we will continue from that point ok.

(Refer Slide Time: 00:35)



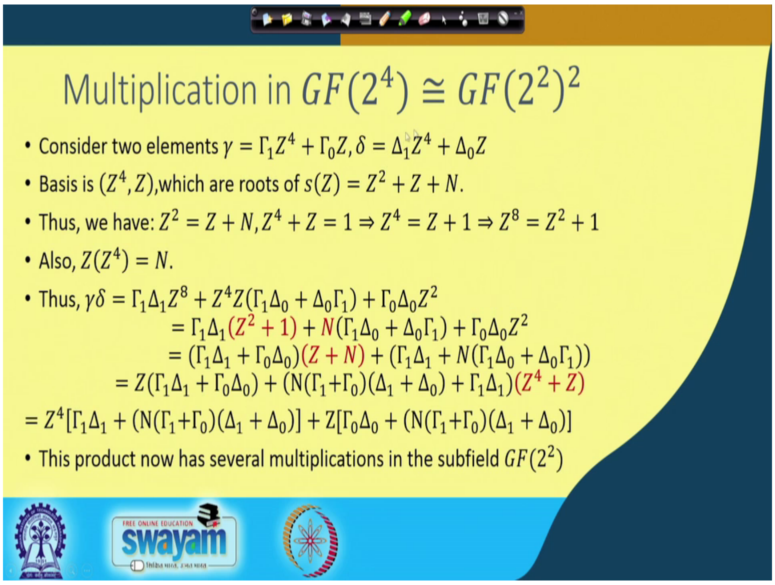
Normal $GF(2^8)$ Inverter

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

So, this is a quick recapitalization of the normal GF 2 power of 4 square inversion circuits, where we were able to decompose my GF 2 power of 4 squared circuits in terms of GF 2 power of 4 computations. So, for example, the multipliers are now in GF 2 power of 4, the inversion is also in GF 2 power of 4 and likewise the scaling. And multiplying that is the scaling operation where you have multiplying with a mu which is a constant is also in GF 2 power of 4.

So, we shall try to see how these individual components can be now worked out.

(Refer Slide Time: 01:07)



Multiplication in $GF(2^4) \cong GF(2^2)^2$

- Consider two elements $\gamma = \Gamma_1 Z^4 + \Gamma_0 Z, \delta = \Delta_1 Z^4 + \Delta_0 Z$
- Basis is (Z^4, Z),which are roots of $s(Z) = Z^2 + Z + N$.
- Thus, we have: $Z^2 = Z + N, Z^4 + Z = 1 \Rightarrow Z^4 = Z + 1 \Rightarrow Z^8 = Z^2 + 1$
- Also, $Z(Z^4) = N$.
- Thus, $\gamma\delta = \Gamma_1\Delta_1 Z^8 + Z^4 Z(\Gamma_1\Delta_0 + \Delta_0\Gamma_1) + \Gamma_0\Delta_0 Z^2$

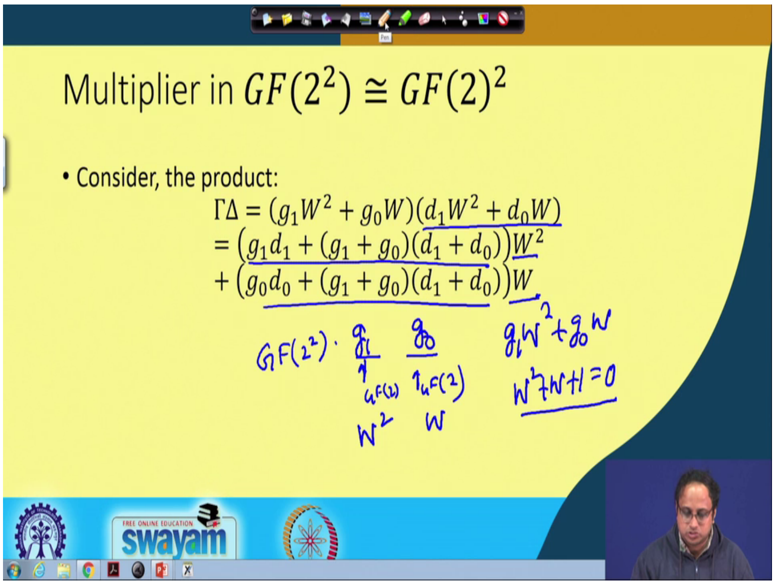
$$= \Gamma_1\Delta_1(Z^2+1) + N(\Gamma_1\Delta_0 + \Delta_0\Gamma_1) + \Gamma_0\Delta_0 Z^2$$
$$= (\Gamma_1\Delta_1 + \Gamma_0\Delta_0)(Z+N) + (\Gamma_1\Delta_1 + N(\Gamma_1\Delta_0 + \Delta_0\Gamma_1))$$
$$= Z(\Gamma_1\Delta_1 + \Gamma_0\Delta_0) + (\mathrm{N}(\Gamma_1 + \Gamma_0)(\Delta_1 + \Delta_0) + \Gamma_1\Delta_1)(Z^4 + Z)$$
$$= Z^4[\Gamma_1\Delta_1 + (\mathrm{N}(\Gamma_1 + \Gamma_0)(\Delta_1 + \Delta_0)] + \mathrm{Z}[\Gamma_0\Delta_0 + (\mathrm{N}(\Gamma_1 + \Gamma_0)(\Delta_1 + \Delta_0)]$$

- This product now has several multiplications in the subfield $GF(2^2)$

We already worked out the product in GF 2 power of 4, essentially where we were able to do multiplication in GF 2 power of 4. The idea was that we will write the element in GF 2 power of 4 as GF 2 power of 2 whole power of 2. And therefore, continue our operations from there ok.

So, now when we see that when you work out this GF 2 power of 4 multiplication then we have got several multiplications which are now in the subfield GF 2 power of 2 ok. So, we should be able to work that also out.

(Refer Slide Time: 01:35)



Multiplier in $GF(2^2) \cong GF(2)^2$

- Consider, the product:

$$\Gamma\Delta = (g_1 W^2 + g_0 W)\underline{(d_1 W^2 + d_0 W)}$$
$$= \big(\underline{g_1 d_1 + (g_1 + g_0)(d_1 + d_0)}\big)\underline{W^2}$$
$$+ \big(\underline{g_0 d_0 + (g_1 + g_0)(d_1 + d_0)}\big)\underline{W}$$

$GF(2^2) \cdot \underset{\underset{GF(2)}{\uparrow}}{\underline{g_1}} \quad \underset{\uparrow GF(2)}{\underline{g_0}}$

$W^2 \quad W$

$g_1 W^2 + g_0 W$

$\underline{W^2 + W + 1 = 0}$

And here is a way how we can do that. When you are doing multiplications in GF 2 power of 2 you can isomorphically write it as relevant in GF 2 power of whole GF 2 power of 2; that means, right there are 2 parts now in the representation. That means, when you are multiplying 2 elements say your elements are gamma and delta; so gamma is an element in GF 2 power of 2. So, when you are doing is multiplication right is that when you essentially these are your corresponding arguments which you have multiplied ok.

So, for example, if you go back and see the equation here then when you are doing this multiplication in GF 2 power of 4 then these elements that is gamma 1 gamma 0 are in GF 2 power of 2 ok. So therefore, right likewise delta 1 and delta 0 are in GF 2 power of 2. So now, you need to do these computations like you know like for example, gamma 1 delta 0; that means you have to multiply in GF 2 power of 2. So, how do you do that is shown here; that means, I take 2 elements in GF 2 power of 2 and I show how to do a multiplication. So, I take a gamma which is in GF 2 power of 2, I take a delta in GF 2 power of 2 and then I multiply them.

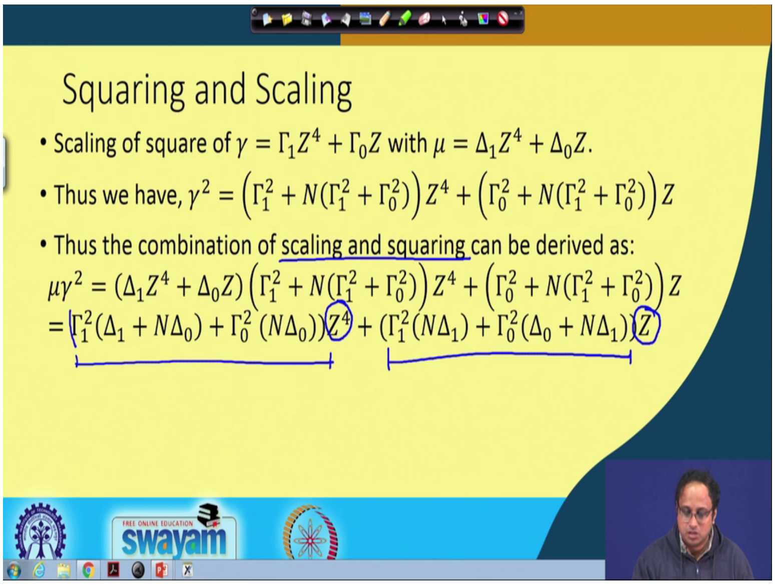
So, again when you are essentially you know like having an element in GF 2 power of 2; that means, if you consider element say you know like in GF 2 power of 2, so that means, right your element has got 2 parts again and each of these elements are now in GF 2. So, this element is in GF 2 this is element is also in GF 2. For example, one element is say g 1 denoted here as g 1 and the other 1 is g g 0, the basis of this is W square and W ok. So therefore, my element is g 1 W square plus g 0 W; likewise my other element is d 1 W square plus d 0 W.

So, when I am multiplying them right essentially I get these elements. I get g 1 g 1 d 1 plus you know I essentially can I am just doing the individual multiplications, and note that I also have this equation that is W square plus W plus 1 is equal to 0 ok. So, essentially I can I will try to use this as my tool for simplification and bring the result back in the original field ok.

So, once you have done that then you essentially get your result back in the original basic that is omega square and omega and these are your corresponding output coefficients. So, if you if you understand these and I leave it you as an exercise to work out the details of how essentially you can simply and being the result back into W square and W ok.

So, therefore, right I have been once. So, if you have understood this right, then we can continue further and see how the next computations can be done.

(Refer Slide Time: 04:21)



Squaring and Scaling

- Scaling of square of $\gamma = \Gamma_1 Z^4 + \Gamma_0 Z$ with $\mu = \Delta_1 Z^4 + \Delta_0 Z$.
- Thus we have, $\gamma^2 = \left(\Gamma_1^2 + N(\Gamma_1^2 + \Gamma_0^2)\right) Z^4 + \left(\Gamma_0^2 + N(\Gamma_1^2 + \Gamma_0^2)\right) Z$
- Thus the combination of scaling and squaring can be derived as:

$$\mu\gamma^2 = (\Delta_1 Z^4 + \Delta_0 Z)\left(\Gamma_1^2 + N(\Gamma_1^2 + \Gamma_0^2)\right) Z^4 + \left(\Gamma_0^2 + N(\Gamma_1^2 + \Gamma_0^2)\right) Z$$
$$= \underbrace{\Gamma_1^2(\Delta_1 + N\Delta_0) + \Gamma_0^2\,(N\Delta_0))}\boxed{Z^4} + \underbrace{(\Gamma_1^2(N\Delta_1) + \Gamma_0^2(\Delta_0 + N\Delta_1))}\boxed{Z}$$

For example, the most important step as I was mentioning is the squaring and the scaling operation in GF 2 power of 4 square. So, note I am doing a scaling with mu. So, mu is my constant which is denoted as delta 1 Z power of 4 plus delta 0 Z and I am doing or applying this scaling on the square of gamma ok. So, the gamma is essentially nothing but gamma 1 Z to the power of 4 plus gamma 0 Z ok. So, this step is essentially this blocks this box that is this box is what we are now trying to expand ok.

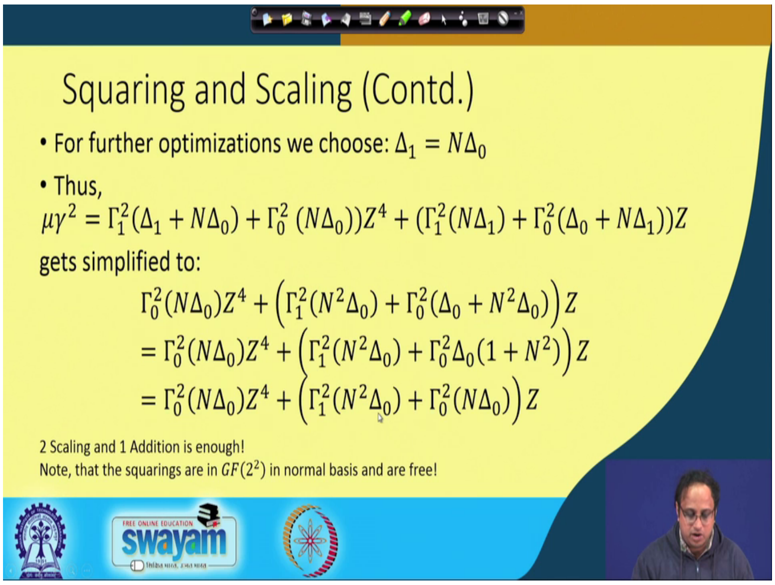
So, if you now want to tell me the details, then that means that when you are doing a gamma square, so, note that gamma is nothing but gamma 1 Z power of 4 plus gamma 0 Z. That means, gamma square essentially can be written in this form ok. So, again I am not going into all the details about how this squaring can be done. But again you know like leave it to you as an exercise to verify, because we have already worked out this product right where we have multiplied for example, we have where we essentially have done this multiplication. So, it is just a simple case where I mean the squaring is nothing but a multiplication where 2 inputs are exactly same ok. So, if you plug in to that right you should get these equations and that and that exact details. I again leave it to you as an exercise, but interestingly we look into the square the scaling operation the scale and squaring operation ok.

So, when you are doing a scaling and squaring operation; that means, you are now multiplying with this constant which is delta 1 Z power of 4 plus delta 0 Z with this output and this is essentially nothing but the squared result ok. Again, if you do a few more few more manipulations then you will see that there are 2 terms here, again one which is a essentially can be expressed in Z power of 4 and Z and these are the 2 components ok.

So, one component is shown here as you know like. So, this is my you know like 1 component and other component is this and you can see that the basis is Z power of 4 and Z. So, again I have written the result of doing a scaling and squaring in my field, because I have been explaining to express that in the original field.

So, now with this is right, we essentially can observe few more interesting things.

(Refer Slide Time: 06:43)



Squaring and Scaling (Contd.)

- For further optimizations we choose: $\Delta_1 = N\Delta_0$
- Thus,

$$\mu\gamma^2 = \Gamma_1^2(\Delta_1 + N\Delta_0) + \Gamma_0^2\,(N\Delta_0))Z^4 + (\Gamma_1^2(N\Delta_1) + \Gamma_0^2(\Delta_0 + N\Delta_1))Z$$

gets simplified to:

$$\begin{aligned}&\Gamma_0^2(N\Delta_0)Z^4 + \left(\Gamma_1^2(N^2\Delta_0) + \Gamma_0^2(\Delta_0 + N^2\Delta_0)\right)Z\\ &= \Gamma_0^2(N\Delta_0)Z^4 + \left(\Gamma_1^2(N^2\Delta_0) + \Gamma_0^2\Delta_0(1 + N^2)\right)Z\\ &= \Gamma_0^2(N\Delta_0)Z^4 + \left(\Gamma_1^2(N^2\Delta_0) + \Gamma_0^2(N\Delta_0)\right)Z\end{aligned}$$

2 Scaling and 1 Addition is enough!

Note, that the squarings are in $GF(2^2)$ in normal basis and are free!

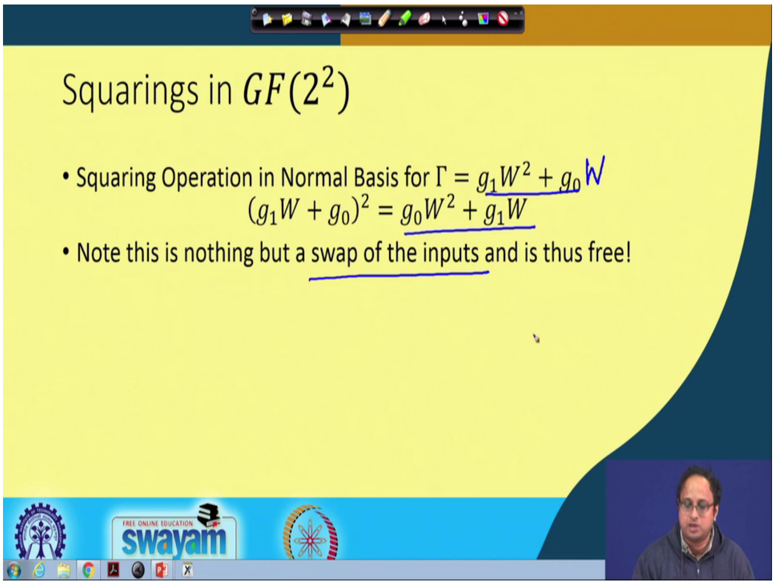
So, to start with when you are doing is optimization and I want to do further more optimizations, let me set delta 1 is equal to N delta 0. Note that the choice of mu is in my hand to some extent. So, if I plug in this optimization that is delta 1 is equal to N delta 0, then you can observe that this mu gamma square essentially had this was my original equation, but then you can observe that this term will vanish, because delta 1 plus N delta 0, because of this optimization will work out to 0 ok.

So therefore, right this will get simplified into this form where you have got you know like delta I mean is you have got delta 0 square multiplied with N I mean gamma 0 square multiplied with N delta 0 Z power of 4 plus this part ok. So now, you note that since delta 1 is equal to N delta 0 and I plug it over here I get N square delta 0 ok. So now, if I take delta 0 common from here I will have got 1 plus N square and note that again N square plus N plus 1 is equal to 0 and therefore, I can substitute 1 plus N square with N ok. So therefore, this is my final form.

So note that, if I want to do this computation I have to do 2 scaling operations. One is a scaling with N; scanning means multiplication with a constant in the lower field and another 1 is the squaring with N square. So, these are my 2 scaling operations that I need to do and I have to do one more addition. So, I have to do one addition here then that is enough ok.

Note that the squarings in GF 2 power of 2, because there are some squarings which you are doing, but now the squarings are is the lower field GF 2 power of 2 GF 2 power of 2 and that is free ok. As I have already kind of inductive in the previous discussions ok.

(Refer Slide Time: 08:37)



Squarings in $GF(2^2)$

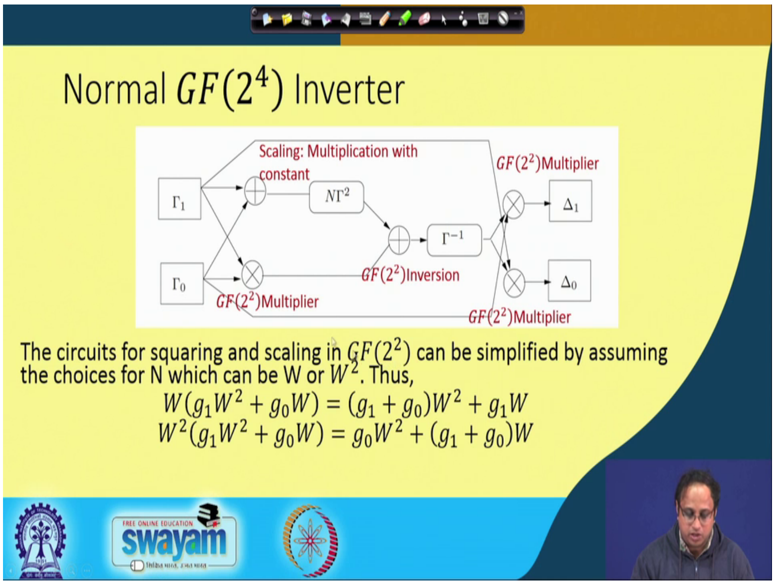
- Squaring Operation in Normal Basis for $\Gamma = g_1W^2 + g_0W$

$$(g_1W + g_0)^2 = g_0W^2 + g_1W$$

- Note this is nothing but a swap of the inputs and is thus free!

Therefore right, you essentially have a pretty compact form of the squaring and the scaling operation, although it is not totally free ok. So therefore, about the same time it is pretty easy to observe. For example, like in you have to see that that the squaring is also free you can easily work that out. So, suppose my input is g 1 W square plus g 0 W. So, again this is missed out. So, you can just correct it by writing this g 0 W. So, if I do a squaring operation then I can work is out as g 0 W square plus g 1 W ok. So, note that if I this is my input and this is my output. Therefore, the square can easily be done by just doing square swapping of the inputs. So, you just need to do a swap and you will get the corresponding output without any explicit computation ok.

(Refer Slide Time: 09:19)



Normal $GF(2^4)$ Inverter

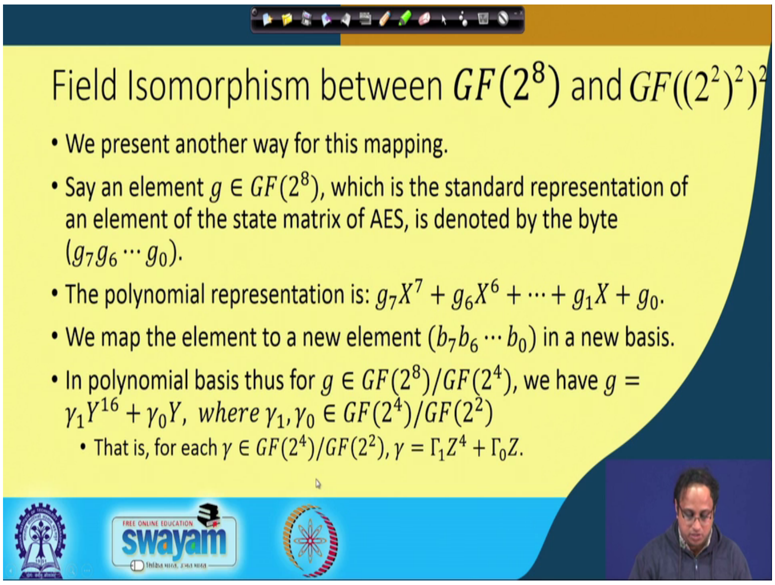
The circuits for squaring and scaling in $GF(2^2)$ can be simplified by assuming the choices for N which can be W or W^2. Thus,

$$W(g_1W^2 + g_0W) = (g_1 + g_0)W^2 + g_1W$$
$$W^2(g_1W^2 + g_0W) = g_0W^2 + (g_1 + g_0)W$$

So, now with this right we should be able to understand how we should now we can again take a look at the lower or the or the GF 2 power of 4 inversion. Again it can be worked out exactly in the same fashion like, but you are seeing previously, but now my computations are or the sub computations are in GF 2 power of 2. So, the circuit for squaring and scaling in GF 2 power 2 can be simplified by assuming the choices of N which can be either W or W squared and I depending upon that you probably have to do scaling with W or a scaling with W square. So, in both cases you can see that whether you are doing a scaling with W or whether you are doing with scaling with W square you essentially have got similar computation which are required ok.

So, therefore, for in 1 case it is just like g 1 plus g 0 W square plus g 1 W. In the other case it is g case it is g 0 W square plus g 1 plus g 0 W ok. So, this is how we can do this part where you are basically doing a scaling with N ok.

(Refer Slide Time: 10:21)



Field Isomorphism between $GF(2^8)$ and $GF((2^2)^2)^2$

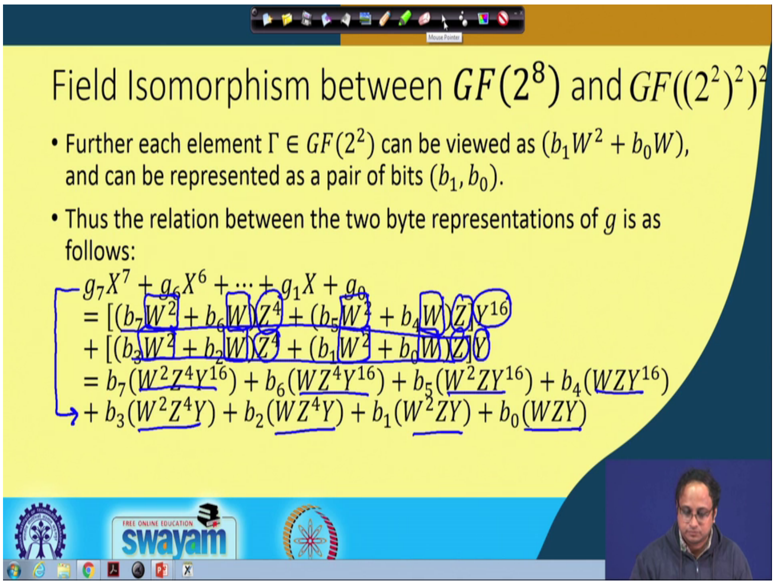
- We present another way for this mapping.
- Say an element $g \in GF(2^8)$, which is the standard representation of an element of the state matrix of AES, is denoted by the byte $(g_7 g_6 \cdots g_0)$.
- The polynomial representation is: $g_7X^7 + g_6X^6 + \cdots + g_1X + g_0$.
- We map the element to a new element $(b_7b_6 \cdots b_0)$ in a new basis.
- In polynomial basis thus for $g \in GF(2^8)/GF(2^4)$, we have $g = \gamma_1 Y^{16} + \gamma_0 Y,\ where\ \gamma_1, \gamma_0 \in GF(2^4)/GF(2^2)$
  - That is, for each $\gamma \in GF(2^4)/GF(2^2), \gamma = \Gamma_1 Z^4 + \Gamma_0 Z$.

So, finally, we essentially have derived out derived all the individual steps and just for completion, we now need to do the final transformation, both from GF 2 power of 8 to GF 2 power of 2 power of 2 2 and from this field back to GF 2 power of 8.

So, we present like in the polynomial basis another way of doing this mapping. So, we taken elements g we belongs to GF 2 power of 8 which is the standard a e s representation. You can abbreviate from by the double from g 0 to g g 7. And therefore, is you have corresponding polynomial representation. In the normal basis when you are mapping this to say b 7 to b 0, then you note that this element that is when you are expressing it as GF 2 power of 4 square will have 2 parts ok.

The first part is a gamma 1 second part is gamma 0. So, my element is gamma 1 Y power of 16 plus gamma 0 Y, likewise these gamma elements I are elements from GF 2 power of 2 whole power of 2. So, I can express them as say capital gamma 1 Z power of 4 plus capital gamma 0 Z and likewise.

(Refer Slide Time: 11:31)



Field Isomorphism between $GF(2^8)$ and $GF((2^2)^2)^2$

- Further each element $\Gamma \in GF(2^2)$ can be viewed as $(b_1W^2 + b_0W)$, and can be represented as a pair of bits (b_1, b_0).
- Thus the relation between the two byte representations of g is as follows:

$$\begin{aligned}
&g_7X^7 + g_6X^6 + \cdots + g_1X + g_0 \\
&= [(b_7\boxed{W^2} + b_6\boxed{W})\boxed{Z^4} + (b_5\boxed{W^2} + b_4\boxed{W})\boxed{Z}]\boxed{Y^{16}} \\
&+ [(b_3\boxed{W^2} + b_2\boxed{W})\boxed{Z^4} + (b_1\boxed{W^2} + b_0\boxed{W})\boxed{Z}]\boxed{Y} \\
&= b_7(\underline{W^2Z^4Y^{16}}) + b_6(\underline{WZ^4Y^{16}}) + b_5(\underline{W^2ZY^{16}}) + b_4(\underline{WZY^{16}}) \\
&+ b_3(\underline{W^2Z^4Y}) + b_2(\underline{WZ^4Y}) + b_1(\underline{W^2ZY}) + b_0(\underline{WZY})
\end{aligned}$$

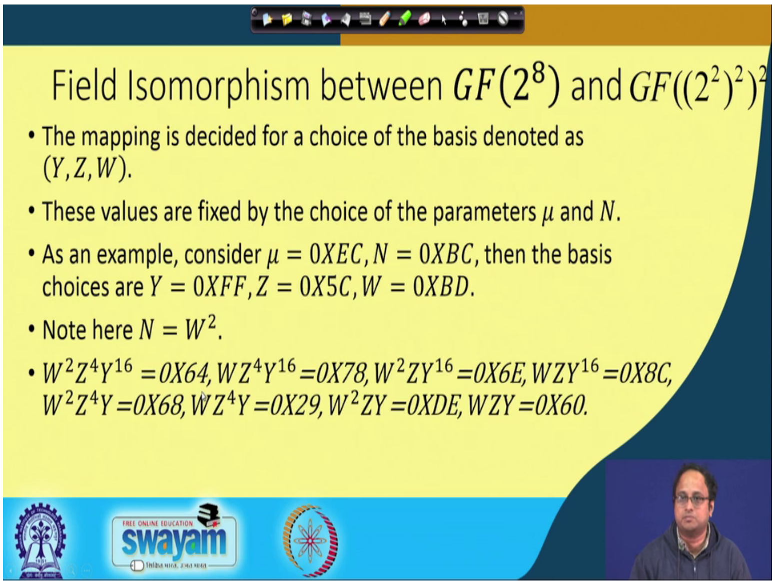
So therefore, right what I can do is now that means, each further more each of these elements, like gamma like gamma they will be are element in GF 2 power of 2. Therefore, I can write that as b 1 you know like I can write that as d 1 or b 1 W square plus b 0 W ok, where each of these b 1 b 0 are my bits or in 0 1 values. So, bringing all of them together; that means, this polynomial is nothing but there are 2 parts you can actually like in equivalent in the converted form actually, you essentially have these 2 parts right.

For example, when I am having this is my higher part and this is my lower part. So, you see that I write this is a basis Y power of 16 and this is my basis Y. And again recursively this part are each of these parts you can write them in the basis Z power of 4 and Z and Z power of 4 and Z. And likewise each of these individual terms you can write as in basis W square W, W square W and so on ok; likewise here also the basis W square W, and likewise, here also the basis W square and W, ok.

So therefore, if you know just product this is this is multiply you will get the coefficient for b 7 as W square Z power of 4 Y power of 16 and so on ok. So that means, now if I want to do a comparison I want to do a kind of you know like conversion then I can use these products for my comparisons. I can get from these coefficients I can get these coefficients by calculating these values. So, if you want to calculate these values you need to know what is your mu and N ok. So, mu and N once they are decided this basis gets fixed exactly like what you have done in the context of polynomial basis ok.

So therefore, I mean let us see how the matrix looks like.

(Refer Slide Time: 13:23)



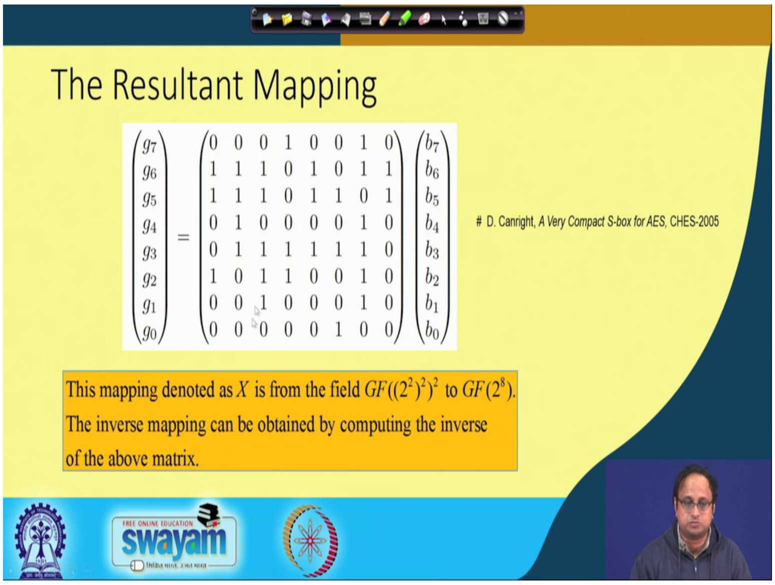
Field Isomorphism between $GF(2^8)$ and $GF((2^2)^2)^2$

- The mapping is decided for a choice of the basis denoted as (Y, Z, W).
- These values are fixed by the choice of the parameters μ and N.
- As an example, consider $\mu = 0XEC, N = 0XBC$, then the basis choices are $Y = 0XFF, Z = 0X5C, W = 0XBD$.
- Note here $N = W^2$.
- $W^2Z^4Y^{16} = 0X64, WZ^4Y^{16} = 0X78, W^2ZY^{16} = 0X6E, WZY^{16} = 0X8C, W^2Z^4Y = 0X68, WZ^4Y = 0X29, W^2ZY = 0XDE, WZY = 0X60.$

So, what we do is now we take the mu. So, again we take the same mu as I show to you why this choice of mu is correct. I showed to you I think while choice of N is correct likewise you can verify the choice of mu is correct. And once you have fix this choice of mu and N you get the value of Y Z and W as shown here. And therefore, right you can actually get the corresponding products in this way ok. So of course, like when you are doing these multiplications you have to take you know like when you are do any modular reduction you can take the AES polynomial for doing the modular reduction ok.

So, again I leave it to as an exercise to verify that indeed you get these values like 6 4 7 8 all of them are in hexadecimal. That means, you can elaborate them as 2 parts and you can write them as in binary format ok.

(Refer Slide Time: 14:15)



The Resultant Mapping

$$\begin{pmatrix} g_7 \\ g_6 \\ g_5 \\ g_4 \\ g_3 \\ g_2 \\ g_1 \\ g_0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix}$$

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

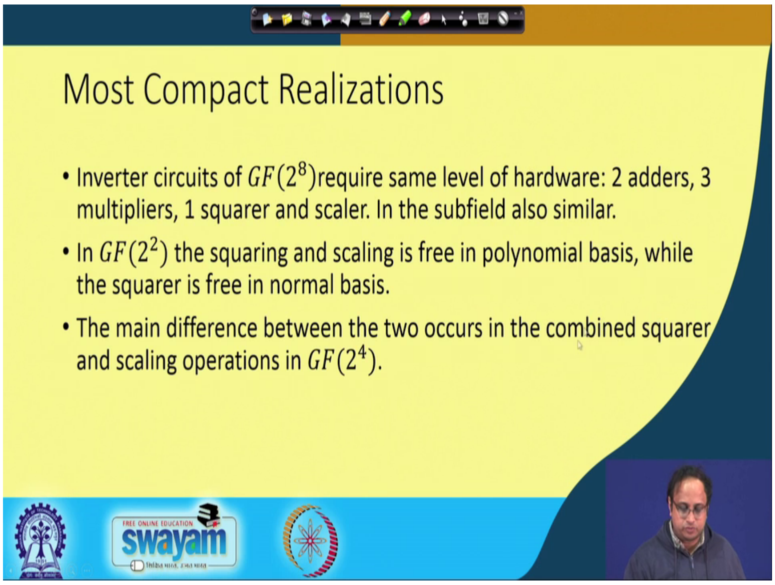
This mapping denoted as X is from the field $GF((2^2)^2)^2$ to $GF(2^8)$. The inverse mapping can be obtained by computing the inverse of the above matrix.

Once you have got these binary equivalents it is straightforward to write this matrix. So, you can see that each of these columns ok. So, basically like what it means is that if you get this that if I am basically multiplying this with the vector denoting b 7 b 6 and so on.

So that means, exactly that is what is in the right hand side of this matrix. So, these matrix multiplies with b 7 to b 0 and get your results in g 7 to g 0. So, we are basically using this matrix mapping an element in the composite field to GF 2 power of 8 ok. So, if I call this mapping rewrite as you know like X inverse then that would so, or may be X basically. So, then the inverse of this mapping we will take me an take me from GF 2 power of 8 to GF 2 power of 2 whole power of 2 whole power of 2 this is the composite field representation ok.

So, you can verify that each of these columns will stand for these constants. For example, this right we will stand for the constant 6 0. So, you can verify that that is that in a straightforward manner that this column essentially, so, this part write stands for 6 and this stand for 0 and therefore, it is nothing but 6 0 ok. So, likewise you can verify the other columns ok, so, which I am not go in to ok.

(Refer Slide Time: 15:41)



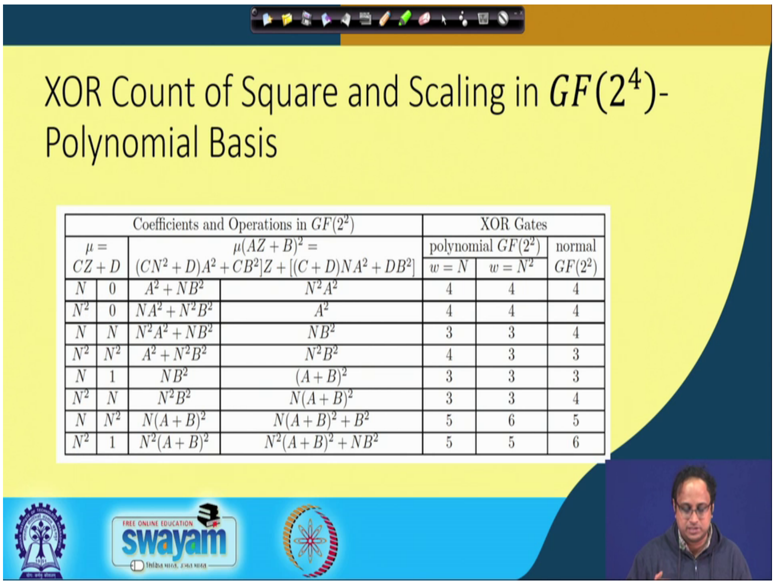
Most Compact Realizations

- Inverter circuits of $GF(2^8)$require same level of hardware: 2 adders, 3 multipliers, 1 squarer and scaler. In the subfield also similar.
- In $GF(2^2)$ the squaring and scaling is free in polynomial basis, while the squarer is free in normal basis.
- The main difference between the two occurs in the combined squarer and scaling operations in $GF(2^4)$.

Now, let us take a look about the comparisons because we have derived quite a number of equations normal basis and polynomial basis. Let us take a final look into how we can compare ok. So therefore, what we are seen is that when we are wanting or try to going to the compact realizations the inversion circuits of GF 2 power of 8 requires roughly the same level of hardware. You will see compare to circuit you will see there are 2 adders 3 multipliers 1 square and scalar. So, that is not much to kind of distinguished from one with the other.

Likewise, in GF 2 power of 2 the squaring and scaling is free in polynomial basis, but the squared is free in the normal basis. So therefore, the main difference actually between the 2 occurs in the combined squaring and scaling operation in GF 2 power of 4 ok.

(Refer Slide Time: 16:31)



XOR Count of Square and Scaling in $GF(2^4)$-Polynomial Basis

Coefficients and Operations in $GF(2^2)$				XOR Gates		
$\mu =$		$\mu(AZ+B)^2 =$		polynomial $GF(2^2)$		normal
$CZ+D$		$(CN^2+D)A^2+CB^2]Z+[(C+D)NA^2+DB^2]$		$w=N$	$w=N^2$	$GF(2^2)$
N	0	A^2+NB^2	N^2A^2	4	4	4
N^2	0	$NA^2+N^2B^2$	A^2	4	4	4
N	N	$N^2A^2+NB^2$	NB^2	3	3	4
N^2	N^2	$A^2+N^2B^2$	N^2B^2	4	3	3
N	1	NB^2	$(A+B)^2$	3	3	3
N^2	N	N^2B^2	$N(A+B)^2$	3	3	4
N	N^2	$N(A+B)^2$	$N(A+B)^2+B^2$	5	6	5
N^2	1	$N^2(A+B)^2$	$N^2(A+B)^2+NB^2$	5	5	6

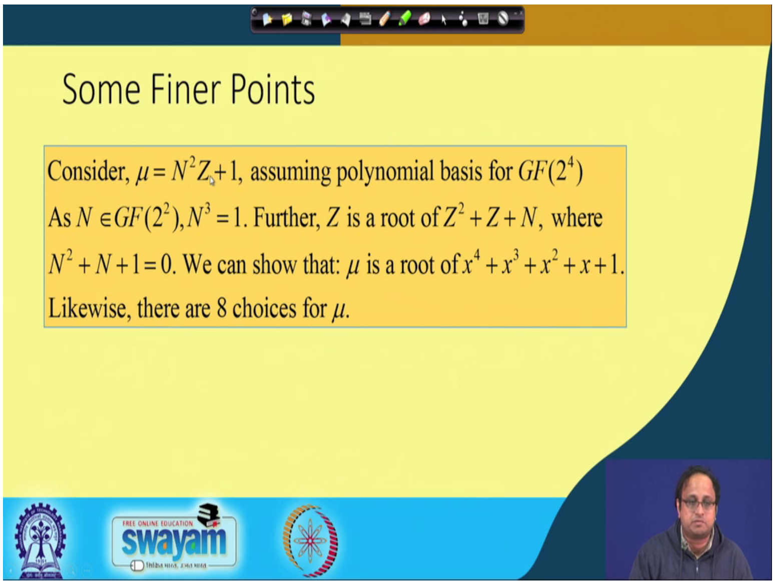
So, let us take look into that operation in more details and here are all the possible descriptions of that and I just enumerate the XOR count, because XOR is the most used gate in these realizations. So, there are 8 choices of mu and I told you why there are 8 choice of mu, because there are 4 4 roots of you know like irreducible polynomials like X to the power of 4 plus X cube plus 1, and likewise the other irreducible polynomial. So, there are 4 roots for each of them and you have got eights are choice ok. And likewise, if you workout the cost for squaring and scaling this is your corresponding equation. Again I leave it as an exercise to verify that it is indeed the correct enumeration or correct elaboration of the equation. These are the 2 outputs; that means, again this is done in the polynomial basis.

So, you can observed that the polynomial is written as AZ plus B because it is in the polynomial basic ok. And likewise you observe that I am trying to basically find out now that what are the cost of these operations ok. When you are doing this computations again you have basically doing it in GF 2 power of you are doing in soft field right, so, basically you are doing in GF 2 power of 2. So, this lower field computation in GF 2 power of 2 you can again do in either polynomial basis or normal basis that is why write we have so many combinations.

If you remember we discuss in the first slide right about when you started this discussion in how many ways you can write the AES S box ok. So, you can actually do a polynomial or a normal basis representation in the lower field as well and depending upon you know like the normal basis we have only have one choice, but in the polynomial basis you have got two choices depending upon the basis ok.

So, the basis either omega or omega square and likewise write you will see that the gate counts are also varying ok. In the normal basis you have got another you know like sort enumeration of number of gates. In particular let me show you with 1 of the example, so, last one. So, N square so, in this case mu is nothing but N square C plus so, C is your N square and delta is 1; that means, the value of mu is this case is N square Z plus 1.

(Refer Slide Time: 18:45)



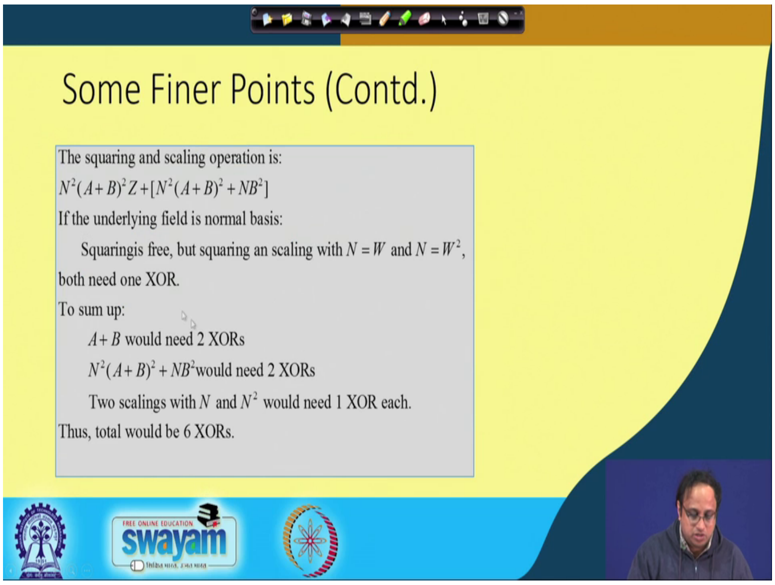
Some Finer Points

Consider, $\mu = N^2Z+1$, assuming polynomial basis for $GF(2^4)$
As $N \in GF(2^2), N^3 = 1$. Further, Z is a root of Z^2+Z+N, where
$N^2+N+1=0$. We can show that: μ is a root of $x^4+x^3+x^2+x+1$.
Likewise, there are 8 choices for μ.

So, if I take that then mu is N square Z plus 1 and assuming that this is a polynomial basis for GF 2 power of 4 and assuming the polynomial basis for GF 2 power of 4. That means, as N belongs to GF 2 power of 2. If remember I said N cube is equal to 1. Further Z is also a root of Z square plus Z plus N ok. So, where you know like N square plus N plus 1 is equal to 0.

So, you can show again I leave it to as an exercise and you can follow it from the text book also that mu will satisfy this equation. That means, mu is a root of the irreducible polynomial in GF 2 power of 4 which is x to the power of 4 plus x to the power of 3 plus x square plus x plus 1. Likewise mu can also be a root of the other irreducible polynomial which is the x to the power of 4 plus x cube plus 1, and that is why that 8 choices of mu ok, one of this choice is say N square Z plus 1 ok.

(Refer Slide Time: 19:43)



Some Finer Points (Contd.)

The squaring and scaling operation is:

$N^2(A+B)^2Z+[N^2(A+B)^2+NB^2]$

If the underlying field is normal basis:

Squaringis free, but squaring an scaling with $N=W$ and $N=W^2$, both need one XOR.

To sum up:

$A+B$ would need 2 XORs

$N^2(A+B)^2+NB^2$would need 2 XORs

Two scalings with N and N^2 would need 1 XOR each.

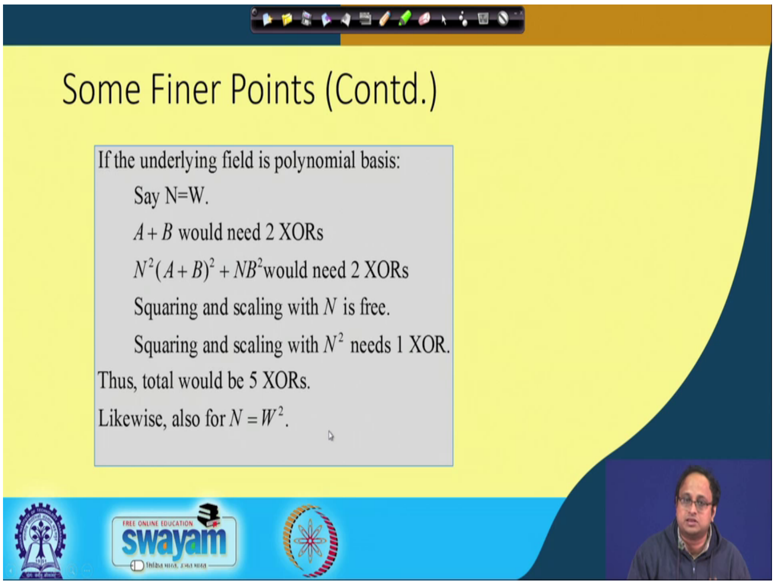
Thus, total would be 6 XORs.

So, with this choice you can actually observe the squaring and scaling operation ok. Again as I said I leave it to as an exercise to verify this equation. I will just show you the enumeration here ok.

So, the enumeration works us follows. If the underlying field is normal basis that means, I am talking about the last column in my table. Then the squarings are free. So, the squaring write are free in the normal basis representation, but a squaring and scaling with N equal to W and with N equal to W square both will required one XOR gates ok. And therefore, to sum up write these competitions like A plus B will take to XORs, because please note that A is an element in GF 2 power of 2. And that means, if you want to do an addition in GF 2 power of 2 you need to XOR gates ok; one for the lower bit, one for the higher bit.

So, you need to XORs here likewise for this operation also for this plus you need to XORs ok. But what is free is the squarings are free, but the scaling is not ok. So, whether you are doing a scaling with N square or whether you are doing a scaling with N you need one XOR each and that is why you need 2 plus 2 plus 2 that is 6 XORs and that is exactly right what we have seen in the table ok.

(Refer Slide Time: 20:55)



Some Finer Points (Contd.)

If the underlying field is polynomial basis:

Say N=W.

$A+B$ would need 2 XORs

$N^2(A+B)^2+NB^2$would need 2 XORs

Squaring and scaling with N is free.

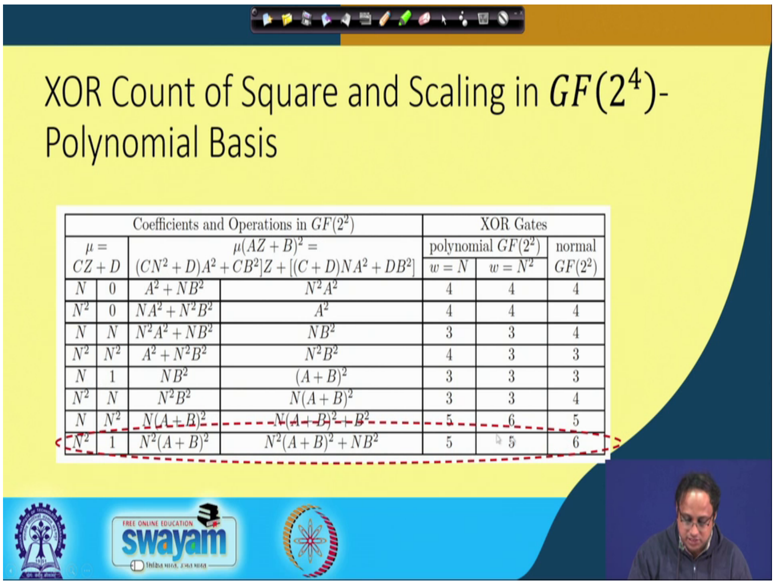
Squaring and scaling with N^2 needs 1 XOR.

Thus, total would be 5 XORs.

Likewise, also for $N=W^2$.

Likewise, the underlining field computation can also be done in the polynomial basis. When you are doing in the polynomial basis you have got 2 choices either N is equal to W or you know like or N equal to W square. So, if you take N equal to W again A plus B on this edition can be done with 4 XORs 2 XORs each, but the squaring and scaling with N is free ok, but the squaring and scaling with N squared with still in 1 XORs. So, you know you need 5 XORs ok. So therefore, you see that in the lower field if it polynomial basis we actually say 1 XOR ok, likewise for N equal to W square.

(Refer Slide Time: 21:33)

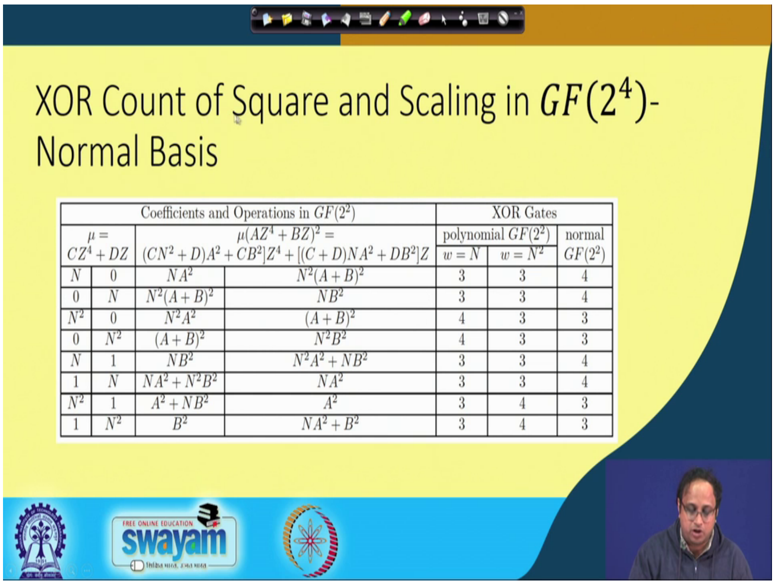


XOR Count of Square and Scaling in $GF(2^4)$-Polynomial Basis

Coefficients and Operations in $GF(2^2)$				XOR Gates		
$\mu =$ $CZ+D$		$\mu(AZ+B)^2 =$ $(CN^2+D)A^2+CB^2]Z+[(C+D)NA^2+DB^2]$		polynomial $GF(2^2)$		normal
				$w=N$	$w=N^2$	$GF(2^2)$
N	0	A^2+NB^2	N^2A^2	4	4	4
N^2	0	$NA^2+N^2B^2$	A^2	4	4	4
N	N	$N^2A^2+NB^2$	NB^2	3	3	4
N^2	N^2	$A^2+N^2B^2$	N^2B^2	4	3	3
N	1	NB^2	$(A+B)^2$	3	3	3
N^2	N	N^2B^2	$N(A+B)^2$	3	3	4
N	N^2	$N(A+B)^2$	$N(A+B)^2+B^2$	5	6	5
N^2	1	$N^2(A+B)^2$	$N^2(A+B)^2+NB^2$	5	5	6

So, that is exactly what we see in this table where if you do this type them in that lower field combination in polynomial basis you required 5 XORs each where is if you do this in normal basis you need 6 XORs ok.

(Refer Slide Time: 21:47)

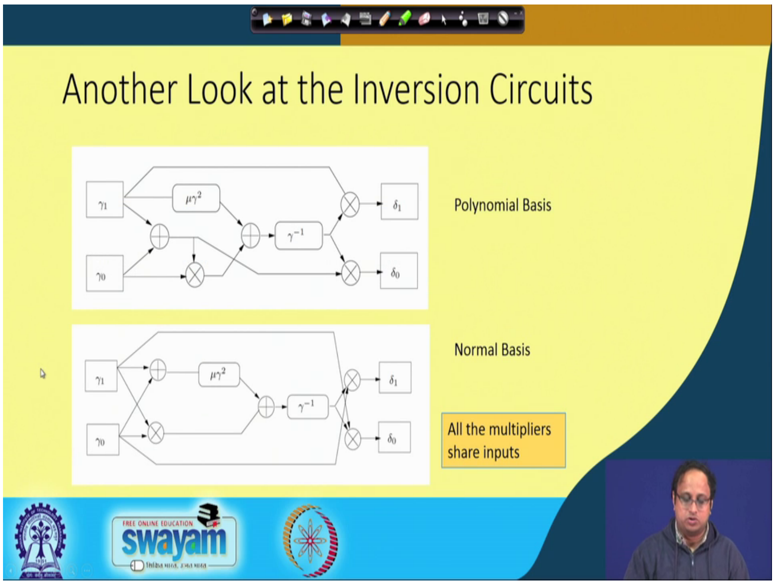


XOR Count of Square and Scaling in $GF(2^4)$-Normal Basis

Coefficients and Operations in $GF(2^2)$				XOR Gates		
$\mu =$ $CZ^4 + DZ$		$\mu(AZ^4 + BZ)^2 =$ $(CN^2 + D)A^2 + CB^2]Z^4 + [(C + D)NA^2 + DB^2]Z$		polynomial $GF(2^2)$		normal $GF(2^2)$
				$w = N$	$w = N^2$	
N	0	NA^2	$N^2(A+B)^2$	3	3	4
0	N	$N^2(A+B)^2$	NB^2	3	3	4
N^2	0	N^2A^2	$(A+B)^2$	4	3	3
0	N^2	$(A+B)^2$	N^2B^2	4	3	3
N	1	NB^2	$N^2A^2 + NB^2$	3	3	4
1	N	$NA^2 + N^2B^2$	NA^2	3	3	4
N^2	1	$A^2 + NB^2$	A^2	3	4	3
1	N^2	B^2	$NA^2 + B^2$	3	4	3

So, likewise right you can work out the XOR counts for squaring and scaling in normal basis and you can see that there is a little bit of advantage when you are doing probably like the competitions in normal basis. There is another very interesting look that you can take the inversion circuits.

(Refer Slide Time: 22:01)



Another Look at the Inversion Circuits

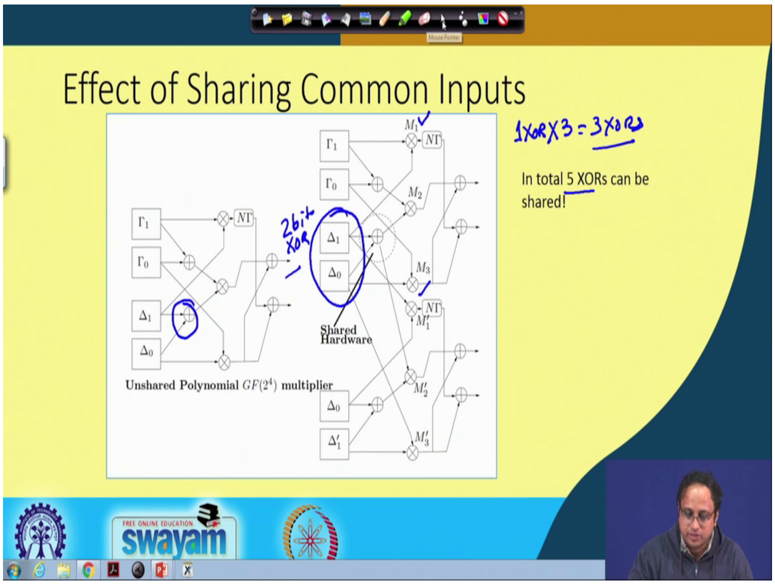
Polynomial Basis

Normal Basis

All the multipliers share inputs

So, here is exactly the polynomial basis inversion and the normal basis inversion net to make main compare. If you see that as I said to you if you just compute the number of computations there is nothing much too kind of compare. It has pretty much the same number of inversions 3, it has got the same number of XORs, same number of inversion, same number of scaling and squaring ok. But interestingly, you see normal basis all the multipliers have got shared inputs, but in polynomial basis if you consider for example, this pair and this pair then they do not have shared inputs ok. So, what is the implication of that? So, if you take a look at the lower field multiplied, so, that field multiplied is in GF 2 power of 4 or GF 2 power of 2 power of 2. So, is basically in GF 2 power of 4 means is in GF 2 power of 2 whole power of 2.

(Refer Slide Time: 22:59)



Effect of Sharing Common Inputs

In total 5 XORs can be shared!

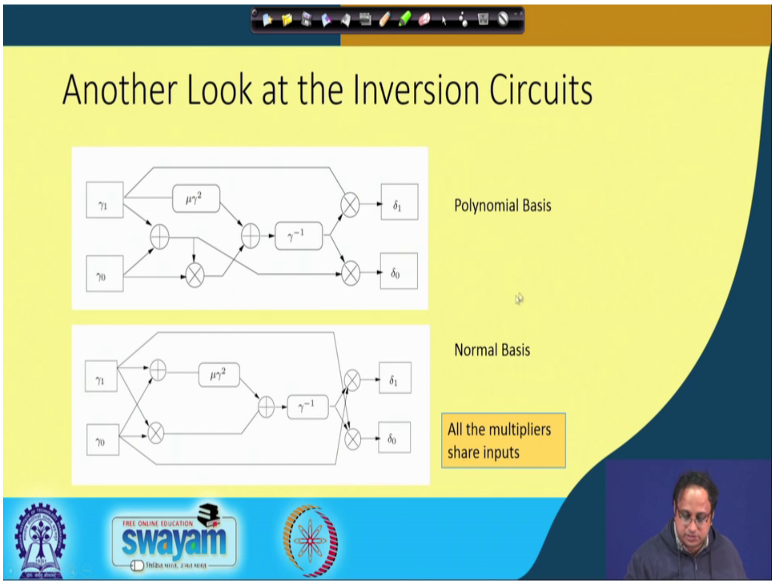
So, then you can easily see that there is an opportunity of saving ok. So, here I have just drawn the GF 2 power of 4 multiplied, but I have drawn 2 copies of GF 2 power of 4 multiplied where one argument is shared ok. So, this is the argument that I have shared. So, you can see that if I share this argument. That means, this is my argument that has been shared, then if you remember right this particular XOR you can actually shared between the 2 competitions. So that means, right you can actually save some gates here ok.

Likewise, you can see that there are free multipliers like one if you observe M 1 and M 1 dash ok, you see that there is also one input with this shared like this is one input and this is one input there essentially coming from the same delta 1. So, you can still save some gates over there ok.

So, in the lower field right you will be saving one get their ok. So, therefore, for each of this computations you will be saving one gate because the lower field lower computation will be in GF 2 2 ok. So, you will be saving this XOR means you will be saving a 1 bit XOR, whereas in this particular field like it is a 2 bit XOR. So, in this diagram this is where you are saving a 2 bit XOR, but if you go down right and consider M 1 and M 1 dash then you are saving one XOR ok, but there are 3 such cases. So, you saved here 1 into 3 which is 3 XORs and therefore, totally you save 3 save 3 plus 2 which is 5 XORs ok.

So therefore, right here you have been opportunity if you have got shared input to save 5 XORs. So now, if you take a like a look back then you will see that so, if I take a look back right then you will see that in the previous circuit right you have if you if you now compare this circuit right you will with this circuit. That means, the polynomial basis circuit with a normal basis circuit.

(Refer Slide Time: 24:47)



Another Look at the Inversion Circuits

Polynomial Basis

Normal Basis

All the multipliers share inputs

In the normal basis circuit you have more opportunities of sharing whereas in this case you can share, but not in one case ok. So therefore, straightaway there is an advantage of 5 XORs in this computation ok.

So, therefore, it turns out that you know like that with all these things right that there are normal basis representation on the top level is probably a good way to get a compact implementation ok. So, all the hard maths pays in terms of gates ok.

(Refer Slide Time: 25:21)

References

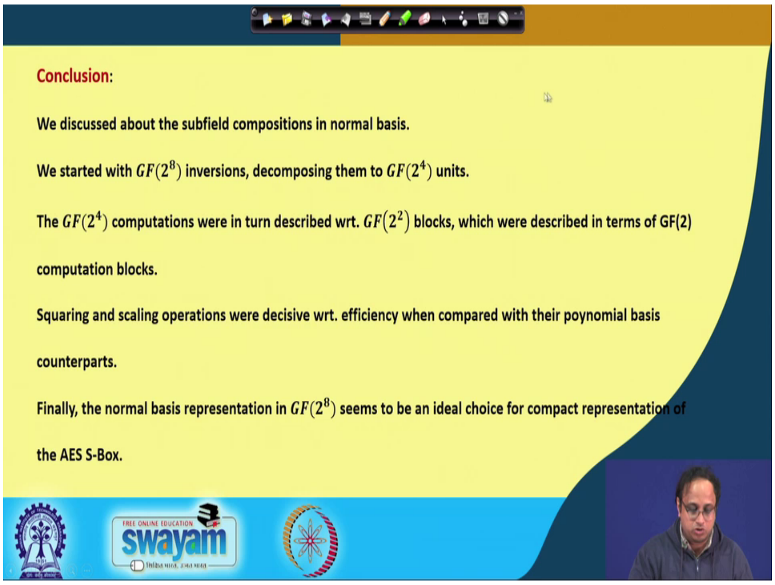
References:

❑ Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, Hardware Security: Design, Threats and Safeguards, CRC Press

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

So, here is like quick reference you can actually go through the original paper of Canright which is published in CHES in 2005. But we have also try to kind of summarize this in the textbook which you can read and probably get more insights about how the design has been done and developed ok.

(Refer Slide Time: 25:41)



Conclusion:

We discussed about the subfield compositions in normal basis.

We started with $GF(2^8)$ inversions, decomposing them to $GF(2^4)$ units.

The $GF(2^4)$ computations were in turn described wrt. $GF(2^2)$ blocks, which were described in terms of GF(2) computation blocks.

Squaring and scaling operations were decisive wrt. efficiency when compared with their poynomial basis counterparts.

Finally, the normal basis representation in $GF(2^8)$ seems to be an ideal choice for compact representation of the AES S-Box.

So, just to conclude we discussed about the subfield composition in normal basis. We started with GF 2 power of 8 inversions decompose them further in GF 2 power of 4 inversions or GF 2 power of 4 computation units. The GF 2 power of 4 computations, were then again in turn you know like describe with respect to GF 2 power of 2 blocks which you are further described in terms of GF 2 computation blocks.

So, we discuss the squaring and scaling operations were decisive with respect efficiency when compared with their polynomial counterparts. And finally, the normal basis representation in GF 2 powder of 8 seems to be an ideal choice for compact representations of the AES S box ok. And in particular right I would also like to mention in the passing that a normal basis representation also probably gives a more fault tolerant design, but that is another story.

With this, I will like to thank you for your attention.