**4.Quotient ring **

The polynomial ,  is not irreducible because  (i.e.  ) is a root of the polynomial . Hence from the Bezout theorem  is divisible by  and  is not irreducible. Then the quotient ring **** is not a field.

Elements of the ring  are polynomials of the degree at most  then can be treated as **** bit words called in the sequel blocks. In Rijndael for example we have ,  and blocks have 32 b length.

Addition + of two polynomials in the ring  is common addition of polynomials along coordinates in  then in fact it is exoring of two **** bit words. As a result addition is simple and fast and can be implemented with one or more logical XOR instructions from arbitrary assembler or a set of two input XOR gates.

Multiplication **\*** of two polynomials in **** is a little more complicated. Assume we have two polynomials:

, where  for every  and

, where  for every 

****

where  denotes common multiplication of polynomials.

Crucial for MRA are the following two theorems 4.1 and 4.2.

**Theorem 4.1** If  and  then for every natural number , and every  we have

 (4.1)

**Proof.** If , then the formula (4.1) is of course true. For  there is  and  , that  and . Dividing the polynomial by the polynomial  for  and taking into account that addition and subtraction of polynomials in  are the same operation we obtain



 







\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_





\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



.

.

.

\_\_\_\_\_\_\_\_\_\_



In other words we have .

Then finally we obtain . ■

**Theorem 4.2**

If we have two polynomials , where  and , , i.e. , where  for every  and

, where  for every 

then the multiplication \* in the quotient ring can be expressed as the following multiplication of matrices:

****

where  is equal to .

**Proof.** The multiplication  in the quotient ring  is defined with the two step formula:

 and 

where multiplication  denotes here common multiplication of polynomials.

The standard homomorphism of the ring of polynomials  into the quotient ring  is given by the formula:



and has the property that for every two polynomials  we have:



or in other words:



Hence we can write:



Common multiplication of polynomials  is from definition a polynomial with coefficients obtained with convolution of two sequences  and . Then we obtain:



where \*’ denotes the convolution. Hence using the theorem 4.1 we have:

 

 



…



…

…………………………………………………………………………………………...

 

 

 

 

…

…

………………………………………………………………………………………………….





 

Hence we have:



(product of the first row of the matrix and the column vector)



(product of the second row of the matrix and the column vector)

,

(product of the third row of the matrix and the column vector)

…,



(product of the *n*-1 row of the matrix and the column vector)



(product of the *n* –row and the column vector)

Then the thesis of the theorem 4.2 is true.**■**

# Remark. The square matrix used in above theorem is a so called circulant matrix. We obtain the circulant matrix rotating the first column *n* times down.

Inverses in the quotient ring are computed with Extended Euclid Algorithm for polynomials or raising an element to be inverted to a power .

The second method is based on the following theorem from group theory.

**Theorem 4.3** If *G* is a finite group then for every element  we have .

**Proof.** Theorem is a direct conclusion from the Lagrange theorem. .**■**

From the above theorem we obtain that .