A new algorithm to find monic irreducible polynomials over extended Galois field GF(p^q) using positional arithmetic.

Sankhanil Dey[1,] Amlan Chakrabarti[2] and Ranjan Ghosh[3],
Institute of Radio Physics and Electronics, 92 A P C Road Kolkata-700009[1,3],
sankhanil12009@gmail.com[1], achakra12@yahoo.com[2], rghosh47@yahoo.co.in[3],
A K Choudhury School of Information Technology, Sector-III, JD-2 block, Kolkata-700098[2],
University of Calcutta[1,2,3].
Corresponding author: Sankhanil Dey, Email: sankhanil12009@gmail.com.

Abstract: Search for monic irreducible polynomials (IPs) over extended Galois field GF(p^q) for a large value of the prime moduli p and a large extension to the Galois Field q is a well needed solution in the field of cryptography. In this paper a new algorithm to obtain monic IPs over extended Galois field GF(p^q) for the large values of p and q is introduced. Here in this paper the positional arithmetic is used to multiply all possible two monic elemental polynomials (EPs) with their Galois field number (GFN) to generate all the monic reducible polynomials (RPs). All the monic RPs are cancelled out from the list of monic basic polynomials (BPs) leaving behind all the monic IPs. Time complexity analysis of the said algorithm is also executed that ensures the algorithm to be less time consuming.

1. Introduction and scope: The Basic Polynomials or BPs over the Galois field GF(p^q) are polynomials with highest degree of terms d equal to the Galois field extension q (d = q) and so it must have (q+1) terms . Elemental Polynomials or EPs are polynomials with highest degree of terms d less than the Galois field extension q (d < q) and so it must have less than (q+1) terms and d varies from 1 through q. BPs with leading co-efficient unity are termed as monic BPs. Monic BPs that do not have two monic EPs rather than constant polynomials (CPs) are termed as monic IPs. The EPs with degree d = 0 are termed as constant polynomials (CPs) and they are p in numbers and not in consideration for this paper. Rests of the monic BPs are the monic reducible polynomials or RPs that must have two non-constant EPs as factors. Generator polynomials or GPs are polynomials with number of terms less than or equal to (q+1) and the code word or generated polynomials from BPs are divisible by GPs but that are also not in consideration for this paper.

There are many algorithms in past that were introduced to find monic IPs over Galois Fields GF(p) and extended Galois fields GF(p^q) for the small values of the prime moduli p as well as the small values of extension q. The hands on computation to find monic IPs over Galois field GF(p^q) for p = 2, q = 2 through 11, p = 3, q = 2 through 7, p = 5, q = 2 through 5 and for p = 7, q = 2 through 4 was initiated by Church [1] in his contribution. The Galois field equivalents of each monic BP for p = 2 through 7 is also reported [1]. Each two monic EPs are multiplied to obtain the RPs. The search for monic IPs ended up with cancellation of all RPs leaving behind the IPs. In Rabin's Algorithm [2] all monic BPs (F(x)) over Galois Field GF(p) of degree n is tested for divisibility with (x^n-x) and the gcd of (F(x), x^{nk_i}-x) where the k_i are all prime divisors of n , to be unity. If any monic BP, F(x) satisfies both condition, the monic BP is termed as monic IP. Later according to Zaman and Ghosh two monic EPs over the Galois field GF(p^q) are multiplied and then divided by all monic BPs over the Galois field GF(p^q) by matrix method. If for any division the residue is 1 then the two monic EPs over the Galois field GF(p^q) are multiplicative inverses (MIs) of each other [3]. In the contribution of Dey and Ghosh the procedure to multiply of GFNs of two polynomials over the Galois field GF(p^q) is illustrated. The each digit of a GFN or the coefficients of each degree term of the polynomial over the Galois field GF(p^q) are multiplied to all digits of other GFN consecutively. Then the obtained digits or coefficients with same degree terms are added and modulated with p to obtain the resultant GFN or the coefficients of the resultant polynomial over the Galois field GF(p^q) [4]. At last according to Dey and Ghosh in this algorithm the decimal equivalents of each of two monic EPs over the Galois field GF(p^q) at a time with highest

degree d and (q-d) where d € {0,..,(q-1)/2} , have been split into the GFNs of each term of two said monic EPs over the Galois field GF(p^q). The coefficients of each term in each two Monic EPs or two GFNs are multiplied, added respectively with each other and modulated to obtain the GFN of the RPs over the Galois field GF(p^q). The DE of the resultant monic BP over the Galois field GF(p^q) is termed as the DE of an RP over the Galois field GF(p^q). The DE of BPs over the Galois field GF(p^q) belonging to the list of RPs over the Galois field GF(p^q) have been cancelled leaving behind the monic IPs over the Galois field GF(p^q) [5].

Now, Here a new multiplication algorithm is introduced to multiply two monic EPs over the Galois field GF(p^q). The procedure is same as decimal multiplication but the each digit in product must be modulated with prime modulus p and the quotient is considered as carry to obtain the result. The multiplicand and multiplier are two GFNs of the two monic EPs over the Galois field GF(p^q). The generation of the GFNs [6] is described in section 2.1 and the procedure and the algorithm is described in section 2.2.

In this algorithm EPs with degree d and q-d where d < q for d = 1,2,…,(q-1)/2 are multiplied over Galois field GF(p^q) through the said multiplication algorithm to ensure the reducibility of the product monic BPs or monic RPs. The left alone BPs or that do not have any factor except CPs and itself are termed as Monic IPs. In this paper for clarity understanding, the pseudo code of the proposed algorithm is presented in Section 3. Time Complexity of the said new algorithm, , Results, Applications of IPs and algorithms and Conclusions are given in sections 4, 5, 6 and 7 respectively. A detailed analysis of the procedure of the algorithm is given in appendix.

2. BCNs and Multiplication algorithm over the Galois field GF(p^q):

Scope: A review work on polynomials is given in section review work. The generation of the GFN is described in subsection 2.1. The procedure and algorithm for the multiplication over the Galois field GF(p^q) of the two GFNs over the said Galois field is illustrated in section 2.2.

Review work:

Short reviews on relevant and related articles are made in this section.

- **Rudolf Church [1935][1].** Here two monic EPs over the Galois field GF(p^q) are multiplied by paper pen to generate all monic RPs over the Galois field GF(p^q). All monic RPs over the Galois field GF(p^q) are cancelled out from the list of the monic BPs over the Galois field GF(p^q) to extract all monic IPs over the Galois field GF(p^q). Here the value of p varies from 2 [q=2 to q=11] to 7 [q=2 to q=4].

- **Zaman et. al [2014][3].** Here two monic EPs over the Galois field GF(p^q) are multiplied and then divided by all monic BPs over the Galois field GF(p^q) by matrix method. If for any division the residue is 1 then the two monic EPs over the Galois field GF(p^q) are multiplicative inverses (MIs) of each other.

- **Dey and Ghosh [2017-a][4].** Here the procedure to multiply of GFNs of two polynomials over the Galois field GF(p^q) is illustrated. The each digit of a GFN or the coefficients of each degree term of the polynomial over the Galois field GF(p^q) are multiplied to all digits of other GFN consecutively. Then the obtained digits or coefficients with same degree terms are added and modulated with p to obtain the resultant GFN or the coefficients of the resultant polynomial over the Galois field GF(p^q).

- **Dey and Ghosh [2017-b][5].** In this algorithm the decimal equivalents of each of two monic EPs over the Galois field GF(p^q) at a time with highest degree d and (q-d) where d € {0,..,(q-1)/2} , have been split into the p-nary coefficients of each term of two said monic EPs over the Galois field GF(p^q). The coefficients of each term in each two Monic EPs or two GFNs are multiplied, added respectively with each other and modulated to obtain the p-nary coefficients of each term of the RPs over the Galois field GF(p^q). The DE of the resultant monic BP over the Galois

field GF(p^q) is termed as the DE of an RP over the Galois field GF(p^q). The DE of BPs over the Galois field GF(p^q) belonging to the list of RPs over the Galois field GF(p^q) have been cancelled leaving behind the monic IPs over the Galois field GF(p^q).

2.1 Generation of the GFNs from the Galois field polynomials over the Galois field GF(p^q).

Coefficient of each degree term of a polynomial are arranged sequentially from highest to lowest degree in a decreasing sequence of degree terms (Coefficient of highest degree term is in MSB and coefficient of lowest degree term is in LSB) to obtain Galois Field Numbers (GFNs) for polynomials over the Galois fields GF(p^q) where p is the prime modulus and q is the extension of the said Galois field. There are two special types of GFNs. Binary Coded Numbers or BCN for polynomials over the Galois field GF(2^q) and Finite Field Numbers (FFNs) for polynomials over finite field GF(p^q) where p is non-prime. Examples of some GFNs, BCNs and FFNs are given in table.1, table.2 and table.3 respectively below and the description of the said tables are also given below.

Row	DEs	Polynomials	BCNs
Col→	1	2	3
1	14406	$6x^4$	60000
2	14407	$6x^4+1$	60001
3	2443	x^4+6x	10060
4	2414	x^4+x+6	10016

Table.1. GFNs of four Galois field polynomials over the Galois field GF(7^4).

Row	DEs	Polynomials	BCNs
Col→	1	2	3
1	16	x^4	10000
2	17	x^4+1	10001
3	18	x^4+x	10010
4	19	x^4+x+1	10011
5	20	x^4+x^2	10100
6	21	x^4+x^2+1	10101
7	22	x^4+x^2+x	10110
8	23	x^4+x^2+x+1	10111
9	24	x^4+x^3	11000
A	25	x^4+x^3+1	11001
B	26	x^4+x^3+x	11010
C	27	x^4+x^3+x+1	11011
D	28	$x^4+x^3+x^2$	11100
E	29	$x^4+x^3+x^2+1$	11101
F	30	$x^4+x^3+x^2+x$	11110
G	31	$x^4+x^3+x^2+x+1$	11111

Table.2. BCNs of 16 Galois field polynomials over the Galois field GF(2^4).

Row	DEs	Polynomials	BCNs
Col→	1	2	3
1	768	$3x^4$	30000

2	770	$3x^4+2$	30002
3	264	x^4+2x	10020
4	267	x^4+2x+3	10023

Table.3. FFNs of four Galois field polynomials over the Galois field GF(4^4).

Description of Table.1, Table.2, and Table.3:

Table.1: Examples of four GFNs over the Galois field GF(7^4) are given in row 1 through 4 of Table.1. DEs of the polynomials, the polynomials itself and the respective GFNs are given in column 1, 2 and 3 of the respective rows.

Table.2: Examples of four BCNs over the Galois field GF(2^4) are given in row 1 through 16 of Table.2. DEs of the polynomials, the polynomials itself and the respective BCNs are given in column 1, 2 and 3 of the respective rows.

Table.3: Examples of four FFNs over the Galois field GF(4^4) are given in row 1 through 4 of Table.3. DEs of the polynomials, the polynomials itself and the respective FFNs are given in column 1, 2 and 3 of the respective rows.

2.2 Procedure and the algorithm for multiplication of the two BCNs over the Galois field GF(p^q).

Here a new multiplication algorithm is introduced to multiply two monic EPs over the Galois field GF(p^q). The procedure is same as decimal multiplication but the each digit in product must be modulated with prime modulus p to obtain the result. The multiplicand and multiplier are two GFNs of the two monic EPs over the Galois field GF(p^q). The procedure is introduced in subsection 2.2.1 and subsection 2.2 is dedicated to algorithm of the said procedure.

2.2.1 Procedure. Let us consider two EPs over Galois field GF(2^4), multiplication of those two EPs over Galois field GF(2^4) must construct a BP. Two EPs over Galois field GF(2^4) are,

EPs	**BCNs or GFNs**
X	0010
x^3+1	1001

Polynomial multiplication of concerned two EPs over Galois field GF(2^4)**:** $x.(x^3+1) = x^4+x$ (BCN = 10010).

Now, by BCNs

A. 1st number. 0010

B. 2nd number. 1001

0010
0000
0000
0010

Product. 0-0-1-0-0-1-0

%-%-%-%-%

2-2-2-2-2

1-0-0-1-0

Product BP = BCN or GFN = 10010 **= polynomial =** x^4+x = Decimal Equivalent = 18.

2.2.2 Algorithm.

The algorithm of multiplication of two polynomials over the Galois field GF(2^4) is given as follows,

Start.

Step 0. Let us take DE of two polynomials A and B over Galois field GF(2^4).

Step 1. Convert two numbers into two BCNs, BCN(A) and BCN(B).

Step 2. Multiply BCN(A) and BCN(B) with decimal multiplication to obtain product P(A×B).
Step 4. Modulate each digit of product with 2 two obtain product BCN of P(A×B).
Stop.

3. Pseudo code for the algorithm to generate all monic IPs over the Galois field GF(p^q):

Scope: the structural description of the algorithm is given in section 3.1. The original pseudocode is given in section 3.2 of this section.

3.1 Structural Description of the Algorithm.

In this algorithm the decimal equivalents of the each of the two monic EPs over the Galois field GF(p^q) at a time with highest degree d and (q-d) where d **€** {0,..,(q-1)/2} , are split into the GFNs of those two monic EPs over the Galois field GF(p^q). The each digit of GFNs of each two monic EPs over the Galois field GF(p^q) is multiplied, added respectively with each other and modulated to obtain the GFN of the obtained monic BP over the Galois field GF(p^q). The DE of the resultant monic BP over the Galois field GF(p^q) is termed as the DE of a reducible monic BP over the Galois field GF(p^q). The DEs of reducible monic BPs over the Galois field GF(p^q) belonging to the list of reducible polynomials are cancelled leaving behind the monic IPs over the Galois field GF(p^q). For the Galois field GF(p^q), where p is the prime modulus and q is the extension of the field, the algorithm is given as follows,

Start.

Step 1: Generate DEs of all the monic EPs, Dec(ep(x)) over the Galois field GF(p^q).

Step 2: Convert Dec(ep(x_1)), Dec(ep(x_2)) with highest degree d and (q-d) respectively where d **€** {0,..,(q-1)/2}, to GFNs of those two monic EPs ep(x_1) and ep(x_2) respectively.

Step 3: Multiply and add terms with degree d **€** {d,d-1,.., 0} and (q-d) **€** {q-d,q-d-1,.., 0} to obtain the decimal coefficients of the each degree terms of the monic BP or each digit of the GFN of the monic BP, BP(x).

Step 4: convert decimal coefficient of each term of monic BP, BP(x) into GFNs.

Step 5: Obtain the DE of the monic BP, BP(x) or Dec(BP(x)) as the DE of a Reducible Polynomial or RP over the Galois field GF(p^q).

Step 6: The DEs of monic BPs belonging to the list of monic RPs are cancelled leaving behind the monic IPs.

Stop.

3.2 Pseudo Code:

```
// Here bp_indx is the DEs of the monic BPs.
// Here ep_indx is the DEs of the monic EPs.
// two monic EPs are multiplied to produce monic RPs or reducible monic BPs.
// All monic RPs are cancelled out produce all monic IPs.
// extn is the extension of the Galois field.
// Multiplication Algorithm is as follows,

for(bp_indx = 0;bp_indx< extn;bp_indx++){
      coeff_bp[bp_indx] = 0;
      for(ep_indx = 0;ep_indx <=indx;ep_indx++){
            if((bp_indx-ep_indx >= 0) && (bp_indx-ep_indx <= extn-indx))
                  coeff_bp[bp_indx]=(coeff_bp[bp_indx]
                  +(coef1_ep[ep_indx]*coef2_ep[bp_indx-ep_indx]))% prime;
      }
}
```

4. Time Complexity of the New Algorithm.

The pseudo code of the algorithm contains two nested loops. The main loop is to test for the concerned BPs and the nested loop is to test for the EPs. So this algorithm have a time complexity of $O(n^2)$. Means it is much faster as Rabin's algorithm [2] for larger value of prime modulus and its modification [2].

Since the time complexity of the both Rabin's algorithm and its modification depends upon the value of prime modulus so it becomes a slow algorithm for large value of the prime modulus. But the new algorithm is much effective and works better as the value of prime modulus and the extension of prime modulus grows larger since time complexity depends only on the value of the extension of the Galois field. So this algorithm is suitable to find monic Irreducible polynomials of higher value of prime modulus and the extension of prime modulus .Comparison of time complexity of the new algorithm with other Algorithms is given below,

Algorithms	**New Algorithm**	**Rabin's Algorithm**	**Rabin's Algorithm(mod)**
Time Complexity	$O(n^2)$	$O(n^4(\log P)^3)$	$0(n^4(\log p)^2 + n^3(\log P)^3)$

5. Results.

The algebraic method or the above pseudo code has been tested on $GF(3^3)$,$GF(7^3)$,$GF(11^3)$, $GF(101^3)$, $GF(3^5)$, $GF(7^5)$, $GF(3^7)$, $GF(7^7)$,. Number of Monic IPs given by this algorithm are same as in hands on calculation by the theorem to count Monic IPs over Galois Field $GF(p^q)$ [8]. The list of numbers of monic IPs for a particular Galois field is given below for all of the eight extended Galois fields. The list of all irreducible monic BPs of $GF(101^3)$ $GF(7^7)$ are given as supplementary material.

Ex.GF.	**$GF(3^3)$**	**$GF(7^3)$**	**$GF(11^3)$**	**$GF(101^3)$**
Number of IPs.	8	112	440	343400
Ex.GF.	**$GF(3^5)$**	**$GF(7^5)$**	**$GF(3^7)$**	**$GF(7^7)$**
Number of IPs.	48	3360	312	117648

6. Applications of the algorithms.

Irreducible polynomials found a permanent seat in generation of crypto 8-bit S-boxes in early days of this century. The first IP over the binary Galois field $GF(2^8)$ is used to generate the elements of the substitution box in Advanced Encryption Standard [7]. IPs over the binary Galois field $GF(2^4)$ are also used to generate crypto 4-bit S-boxes later [6]. The irreducible polynomials with large values of prime p and extension q can also be used to generate crypto 4-bit, 8-bit, 32 bit as well as 64 bit S-boxes in the same manner. The generation of IPs with large value of p and q will break the ice of generation of secure and reliable crypto 4-bit, 8-bit, 32 bit as well as 64 bit S-boxes in computer cryptography. So it is very lucrative to modern cryptographers.

7. Conclusion.

To the best knowledge of the present authors, there is no mention of a paper in which the composite polynomial method is translated into an algorithm and turn into a computer program. The new algorithm is a much simpler to find monic IPs over Galois field $GF(p^q)$. It is able to determine decimal equivalents of the monic IPs over Galois field with a large value of prime modulus, also with large extensions of the prime modulii. So this method can reduce the time complexity to find monic Irreducible Polynomials over Galois field with large value of prime moduli and also with large extensions of the prime moduli. So this would help the crypto community to build S-Boxes or ciphers using irreducible polynomials over Galois Fields with a large value of prime moduli, also with the large extensions of the prime moduli.

References:

[1] Church R., "Tables of Irreducible Polynomials for the first four Prime Moduli", Annals of Mathematics, Vol. 36(1), pp. 198 – 209, January, 1935.

[2] Jacques C'almet And Riidiger Loos, "An Improvement of Rabin's Probabilistic Algorithm For Generating Irreducible Polynomials Over Gf(P)", Information Processing Letters, 20 October 1980, Volume 11, No. 2.

[3] JKM Sadique Uz Zaman, Sankhanil Dey, Ranjan Ghosh, (2015) An Algorithm to find the Irreducible Polynomials over Galois Field GF(p^m), International Journal of Computer Applications 109(15):24-29, DOI:10.5120/19266-1012.

[4] Sankhanil Dey and Ranjan Ghosh, (2017) A new mathematical method to search irreducible polynomials using decimal equivalents of polynomials over Galois field GF(p^q), Journal: Circulation in Computer Science, Vol.2, No.11. pp-17-22, CSL Press, New York, DOI, ISSN. 2456-3692. **https://doi.org/10.22632/ccs-2017-252-68**.

[5] Sankhanil Dey. and Ranjan Ghosh. (2018) Search for Monic Irreducible Polynomials with Decimal Equivalents of Polynomials over Galois Field GF(p^q). Open Journal of Discrete Mathematics, Scientific Research Publishers, 8 (1), 21-33, ISSN online. 2161-7643 ISSN online. 2161-7635. **https://doi.org/10.4236/ojdm.2018.81003**.

[6] Sankhanil Dey, Amlan Chakrabarti , Ranjan Ghosh . (2019) 4-bit crypto S-boxes: Generation with irreducible polynomials over Galois field GF(2^4) and cryptanalysis., International Journal of Tomography and Simulation, ISSN: 2319-3336, Vol. 32, Issue No. 3, CESER publication.

[7] Joan Daemen,Vincent Rijmen (2000), AES Proposal: Rijndael,http://csrc.nist.gov/encryption/aes/ Last Visited: 7th February 2001.

Appendix:

1. A Brief description on evaluation of the monic Basic polynomials (BPs), monic Elemental Polynomials (EPs) and a hands on calculation of the monic reducible polynomials (RPs) and Irreducible polynomials (IPs) over Galois field GF(2^4).

1.1 Basic polynomials (BPs) over Galois field GF(2^4). Polynomials over Galois field GF(2^4) with degree of highest degree term 4 is termed as basic polynomials or BPs over Galois field GF(2^4). Total number of terms in BPs are (4+1 = highest degree +1= extension of Galois field +1 =) 5. For Galois field GF(2^4) the table of BPs with their decimal equivalents (DEs), polynomial presentation and binary coded number (BCN) [Number obtained from coefficients considering highest degree term as MSB and lowest degree term as LSB and also coefficients of terms absent are 0] presentation are given in table.1. The range of DEs of BPs over Galois field GF(2^4) is ($2^4 \leq DE \leq 2^5-1$) $16 \leq DE \leq 31$, and total number of BPs are (2^4=) 16.

Table.1. List of BPs over Galois field GF(2^4)

Row	DEs	Polynomials	BCNs
1	16	x^4	10000
2	17	x^4+1	10001
3	18	x^4+x	10010
4	19	x^4+x+1	10011
5	20	x^4+x^2	10100
6	21	x^4+x^2+1	10101
7	22	x^4+x^2+x	10110
8	23	x^4+x^2+x+1	10111
9	24	x^4+x^3	11000
A	25	x^4+x^3+1	11001
B	26	x^4+x^3+x	11010
C	27	x^4+x^3+x+1	11011
D	28	$x^4+x^3+x^2$	11100
E	29	$x^4+x^3+x^2+1$	11101
F	30	$x^4+x^3+x^2+x$	11110
G	31	$x^4+x^3+x^2+x+1$	11111

1.2 Elemental polynomials (EPs) over Galois field GF(2^4). Polynomials over Galois field GF(2^4) with degree of highest degree term less than 4 is termed as elemental polynomials or EPs over Galois field GF(2^4). Maximum number of terms in EPs are (4 = highest degree= extension of Galois field) 4 and minimum 1. For Galois field GF(2^4) the table of EPs with their decimal equivalents (DEs), polynomial presentation and binary coded number (BCN) [Number obtained from coefficients considering highest degree term as MSB and lowest degree term as LSB and also coefficients of terms absent are 0] presentation are given in table.1. The range of DEs of EPs over Galois field GF(2^4) is ($0 \leq DE \leq 2^4$) $0 \leq DE \leq 15$, and total number of BPs are (2^4=) 16. The polynomials 0 [00000] and 1[00001] are termed as constant polynomials or CPs over Galois field GF(2^4) since they carries only constant terms in it. They are not in our interest in this study.

Table.2. List of EPs over Galois field GF(2^4)

Row	DEs	Polynomials	BCNs
1	0	0	00000
2	1	1	00001
3	2	X	00010
4	3	x+1	00011
5	4	x^2	00100
6	5	x^2+1	00101
7	6	x^2+x	00110
8	7	x^2+x+1	00111
9	8	x^3	01000
A	9	x^3+1	01001
B	10	x^3+x	01010
C	11	x^3+x+1	01011
D	12	x^3+x^2	01100
E	13	x^3+x^2+1	01101
F	14	x^3+x^2+x	01110
G	15	x^3+x^2+x+1	01111

1.3 Reducible polynomials (RPs) and Irreducible Polynomials (IPs) over Galois field GF(2^4). Reducible polynomials have two non-constant EPs as its factor. Polynomial multiplication of two EPs must be an RP. Rests of polynomials that have it self and constant polynomials as factor are termed as irreducible polynomials or IPs. In table.3. below all reducible polynomials are listed in column RPs and DEs of RPs are listed in column DEs (RPs) with their BCNs in column BCNs (RPs). The corresponding two non-constant EP factors are given in column Factors. BPs that are not present in the table follows are IPs and here DE of IPs are 19, 25, 31 i.e. they are 3 in number.

Row	Factors	RPs	DEs (RPs)	BCNs (RPs)
1	x. x^3	x^4	16	10000
2	x. (x^3+1)	x^4+x	18	10010
3	x. (x^3+x)	x^4+x^2	20	10100
4	x. (x^3+x+1)	x^4+x^2+x	22	10110
5	x. (x^3+x^2)	x^4+x^3	24	11000
6	x. (x^3+x^2+1)	x^4+x^3+x	26	11010
7	x. (x^3+x^2+x)	x^4+x^3+x^2	28	11100
8	x. (x^3+x^2+x+1)	x^4+x^3+x^2+x	30	11110
9	(x+1). x^3	x^4+x^3	24	11000
10	(x+1). (x^3+1)	x^4+x^3+x+1	27	11101
11	(x+1). (x^3+x)	x^4+x^3+x^2+x	30	11110
12	(x+1). (x^3+x+1)	x^4+x^3+x^2+1	29	11101
13	(x+1). (x^3+x^2)	x^4+x^2	20	10100

14	$(x+1).(x^3+x^2+1)$	x^4+x^2+x+1	23	10111
15	$(x+1).(x^3+x^2+x)$	x^4+x	18	10010
16	$(x+1).(x^3+x^2+x+1)$	x^4+1	17	10001
17	$x^2.x^2$	x^4	16	10000
18	$x^2.(x^2+1)$	x^4+x^2	20	10100
19	$x^2.(x^2+x)$	x^4+x^3	24	11000
20	$x^2.(x^2+x+1)$	$x^4+x^3+x^2$	28	11100
21	$(x^2+1).(x^2+1)$	x^4+1	17	10001
22	$(x^2+1).(x^2+x)$	$x^4+x^3+x^2+x$	30	11110
23	$(x^2+1).(x^2+x+1)$	x^4+x^3+x+1	27	11011
24	$(x^2+x).(x^2+x)$	x^4+x^2	20	10100
25	$(x^2+x).(x^2+x+1)$	x^4+x	18	10010
26	$(x^2+x+1).(x^2+x+1)$	x^4+x^2+1	21	10101

Table.3. List of RPs over Galois field GF(2^4).

List of IPs over Galois field GF(2^4) is given in table 4. Below,

Row	Irreducible Polynomials (IPs)	DE of IPs	BCN(IPs)
1	x^4+x+1	19	10011
2	x^4+x^3+1	25	11001
3	$x^4+x^3+x^2+x+1$	31	11111

Table.4. List of IPs over Galois field GF(2^4).