Scientific Research Publishing

Open Journal of Discrete Mathematics, 2018, 8, 21-33
http://www.scirp.org/journal/ojdm
ISSN Online: 2161-7643
ISSN Print: 2161-7635

Search for Monic Irreducible Polynomials with Decimal Equivalents of Polynomials over Galois Field $GF(p^q)$

Sankhanil Dey, Ranjan Ghosh

Institute of Radio Physics and Electronics, University of Calcutta, Kolkata, India
Email: sdrpe_rs@caluniv.ac.in, rghosh47@yahoo.co.in

How to cite this paper: Dey, S. and Ghosh, R. (2018) Search for Monic Irreducible Polynomials with Decimal Equivalents of Polynomials over Galois Field $GF(p^q)$. *Open Journal of Discrete Mathematics*, **8**, 21-33.
https://doi.org/10.4236/ojdm.2018.81003

Received: November 6, 2017
Accepted: January 26, 2018
Published: January 29, 2018

Abstract

Substitution boxes or S-boxes play a significant role in encryption and decryption of bit level plaintext and cipher-text respectively. Irreducible Polynomials (IPs) have been used to construct 4-bit or 8-bit substitution boxes in many cryptographic block ciphers. In Advance Encryption Standard, the elements of 8-bit S-box have been obtained from the Multiplicative Inverse (MI) of elemental polynomials (EPs) of the 1st IP over Galois field $GF(2^8)$ by adding an additive element. In this paper, a mathematical method and the algorithm of the said method with the discussion of the execution time of the algorithm, to obtain monic IPs over Galois field $GF(p^q)$ have been illustrated with example. The method is very similar to polynomial multiplication of two polynomials over Galois field $GF(p^q)$ but has a difference in execution. The decimal equivalents of polynomials have been used to identify Basic Polynomials (BPs), EPs, IPs and Reducible polynomials (RPs). The monic RPs have been determined by this method and have been cancelled out to produce monic IPs. The non-monic IPs have been obtained with multiplication of α where $\alpha \in GF\left(p^q\right)$ and assume values from 2 to $(p-1)$ to monic IPs.

Keywords

Finite Fields, Galois Fields, Irreducible Polynomials, Decimal Equivalents

1. Introduction

Substitution box or S-box in block ciphers is of utmost importance in Public Key Cryptography from the initial days. A 4-bit S-box has been defined as a box of $2^4 = 16$ elements Varies from 0 to F in hex, arranged in a random manner as

*Monic polynomials over Galois field GF(p^q).

used in Data Encryption Standard or DES [1] [2] [3] [4]. Similarly for 8 bit S-box, the number of elements is 2^8 or 256, varying from 0 to 255 as used in Advance Encryption Standard or AES [5] [6]. So the construction of S-boxes is a major issue in Cryptology from initial days. Using Irreducible Polynomials to construct S-box had already adopted by crypto community. But the study of IPs has been limited to almost binary Galois field GF(2^q) as used in AES S-boxes [5] [6]. So the search for monic as well as mon-monic IPs has been the untouched stone to break in cryptography.

Now Basic Polynomials or BPs over Galois Field $GF(p^q)$ have been defined as the polynomials with highest degree q. The polynomials with degree less than q have been termed as Elemental Polynomials or EPs over Galois Field $GF(p^q)$. The polynomials that contain only constant term have been termed as Constant Polynomials or CPs over Galois Field $GF(p^q)$. BPs that have more than one non-constant BPs as Factors have been termed as Reducible Polynomials or RPs over Galois Field $GF(p^q)$. Rest of BPs that have CPs and itself as factors have been termed as Irreducible Polynomials or IPs over Galois Field $GF(p^q)$. BPs with coefficient of highest degree term or leading coefficient equal to unity have been termed as Monic BPs and rest with leading coefficient greater than unity have been termed as Non-Monic BPs as follows.

A basic polynomial $BP(x)$ over finite field or Galois Field $GF(p^q)$ is expressed as,

$$BP(x) = a_q x^q + a_{q-1} x^{q-1} + \cdots + a_q x + a_0.$$

$B(x)$ has $(q+1)$ terms, where a_q has been non-zero and has been termed as the leading coefficient. A BP has been monic if a_q is unity, else it is non-monic. The $GF(p^q)$ have $(p^q - p)$ elemental polynomials $ep(x)$ ranging from p to $(p^q - 1)$ each of whose representation involves q terms with leading coefficient a_{q-1}. The expression of $ep(x)$ is written as,

$$ep(x) = a_{q-1} x^{q-1} + \cdots + a_1 x + a_0,$$

where a_1 to a_{q-1} have not been simultaneously zero.

Many of $BP(x)$, which has an non-constant elemental polynomial as a factor under $GF(p^q)$, have been termed as reducible. Those of the $BP(x)$ that have no factors have been termed as irreducible polynomials $IP(x)$ and has been expressed as,

$$IP(x) = a_q x^q + a_{q-1} x^{q-1} + \cdots + a_q x + a_0 \quad \text{where } a_q \neq 0.$$

In Galois field $GF(p^q)$, the decimal equivalents or DEs of BPs vary from p^q to $(p^{q+1} - 1)$ while the EPs have been those with decimal equivalents vary from p to $(p^q - 1)$. Some of the monic BPs have been irreducible, since they have no monic non-constant EPs as a factor.

The method in this paper has been to look for the DEs of monic RPs with multiplication, addition and modulus of p-nary coefficients of each term of each two monic EPs to obtain the DE of monic RP. The polynomials belonging to the

list of RPs have been cancelled leaving behind the monic IPs. A non-monic IP has been computed by multiplying a monic IP by α where $\alpha \in GF(p)$ and assumes values from 2 to $(p-1)$. In literatures, 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 in turned into a computer program.

The survey of relevant Literatures has been notified in Sec. 2. For convenient understanding, the proposed mathematical method is presented in Sec. 3 for $p = 7$ with $q = 7$. The method can find all monic and after it all non-monic IPs $IP(x)$ over $GF(7^7)$. Sec. 4 demonstrates the obtained results and a discussion on efficiency of the algorithm to show that the proposed searching algorithm is actually able to search for any extension of the Galois field with any prime over Galois field $GF(p^q)$, where $p = 3,5,7,\cdots,101,\cdots,p$ and $q = 2,3,5,7,\cdots,101,\cdots,q$. In Sec. 5 and Sec. 6, the conclusion of the paper and the references have been illustrated. The complete Lists of all monic IPs in a sequential manner over Galois fields GF(7^7) and (101^3) have been found in ref. [7] [8] respectively.

2. Literature Survey

In early Twentieth Century Radolf Church initiated the search for irreducible polynomials over Galois Field $GF(p^q)$ for p = 2, 3, 5 and 7 and for p = 2, q = 1 through 11, for p = 3, q = 1 through 7, for p = 5, q = 1 through 4 and for p = 7, q = 1 through 3 respectively. A manual polynomial multiplication among respected EPs gives RPs in the said Galois field. All RPs have been cancelled from the list of BPs to give IPs over the said Galois field $GF(p^q)$ [9]. Later the necessary condition for a BP to bean IPs had been generalized to Even 2 characteristics. It had also been applied to RPs and gives Irreducible factors mod 2 [10]. Next to it Elementary Techniques to compute over finite Fields or Galois Field $GF(p^q)$ had been descried with proper modifications [11]. In next the factorization of Polynomials over Galois Field $GF(p^q)$ had been elaborated [12]. Later Appropriate Coding Techniques of Polynomials over Galois Field $GF(p^q)$ had been illustrated with example [13]. The previous idea of factorizing Polynomials over Galois Field $GF(p^q)$ [12] had also been extended to Large value of P or Large Finite fields [14]. Later Few Probabilistic Algorithms to find IPs over Galois Field $GF(p^q)$ for degree q had been elaborated with example [15]. Later Factorization of multivariate polynomials over Galois fields $GF(p)$ had also been introduced to mathematics community [16]. With that the separation of irreducible factors of BPs [17] had also been introduced later [18]. Next to it the factorization of BPs with Generalized Reimann Hypothesis (GRH) had also been elaborated [19]. Later a Probabilistic Algorithm to find irreducible factors of Basic bivariate Polynomials over Galois Field $GF(p^q)$ had also been illustrated [20]. Later the conjectural Deterministic algorithm to find primitive elements and relevant primitive polynomials over binary Galois Field $GF(2)$ had been introduced [21]. Some new algorithms to find IPs over Galois Field $GF(p)$ had also been introduced at the same time [22]. Another use of Generalized Reimann

Hypothesis (GRH) to determine irreducible factors in a deterministic manner and also for multiplicative subgroups had been introduced later [23]. The table binary equivalents of binary primitive polynomials had been illustrated in literature [24]. The method to find roots of primitive polynomials over binary Galois field $GF(2)$ had been introduced to mathematical community [25]. A method to search for IPs in a Random manner and factorization of BPs or to find irreducible factors of BPs in a random fashion had been introduced later [26]. After that a new variant of Rabin's algorithm [27] had been introduced with probabilistic analysis of BPs with no irreducible factors [28]. Later a factorization of univariate Polynomials Over Galois Field $GF(p)$ in sub quadratic execution time had also been notified [29]. Later a deterministic algorithm to factorized IPs over one variable had also been introduced [30]. An algorithm to factorize bivariate polynomials over Galois Field $GF(p)$ with hensel lifting had also been notified [31]. Next to it an algorithm had also been introduced to find factor of Irreducible and almost primitive polynomials over Galois Field $GF(2)$ [32]. Later a deterministic algorithm to factorize polynomials over Galois Field $GF(p)$ to distinct degree factors had also been notified [33]. A detailed study of multiples and products of univariate primitive polynomials over binary Galois Field $GF(2)$ had also been done [34]. Later algorithm to find optimal IPs over extended binary Galois Field $GF(2^m)$ [35] and a deterministic algorithm to determine Pascal Polynomials over Galois Field GF(2) [36] had been added to literature. Later the search of IPs and primitive polynomials over binary Galois Field $GF(2)$ had also been done successfully [37]. at the same time the square free polynomials had also been factorized [38] where a work on divisibility of trinomials by IPs over binary Galois Field $GF(2)$ [39] had also been notified. Later a probabilistic algorithm to factor polynomials over finite fields had been introduced [40]. An explicit factorization to obtain irreducible factors to obtain for cyclotomic polynomials over Galois Field $GF(p^q)$ had also been reported later [41]. A fast randomized algorithm to obtain IPs over a certain Galois Field $GF(p^q)$ had been notified [42]. A deterministic algorithm to obtain factors of a polynomial over Galois field $GF(p^q)$ had also been notified at the same time [43]. A review of construction of IPs over finite fields and algorithms to Factor polynomials over finite fields had been reported to literature [44] [45]. An algorithm to search for primitive polynomials had also been notified at the same time [46]. The residue of division of BPs by IPs must be 1 and this reported to literature a bit later [47]. The IPs with several coefficients of different categories had been illustrated in literature a bit later [48]. The use of zeta function to factor polynomials over finite fields had been notified later on [49] At last Integer polynomials had also been described with examples [50].

3. Mathematical Method to Search for Monic IPs over Galois Field $GF(p^q)$

In this section the overview of the method behind the proposed algorithm has

been given in subsec. 2.1. The example to search for monic IPs over Galois field $GF(7^7)$ has been described in subsec. 2.2. The pseudo code of the proposed algorithm of proposed mathematical method has been given in subsec. 3.3 and its time complexity and comparison of time complexity with other algorithms have been illustrated in subsec. 3.4.

3.1. Overview of the Method

The idea behind this mathematical method and is algorithm has been to choose any two non-constant monic EPs at a time split the respective DEs into p-nary coefficients of respective EPs. Two EPs have been multiplied through polynomial multiplication or multiplication by the said method to obtain a BP. Since the obtained BP has two non-constant EPs as factors so it is termed as monic RPs. After considering all possible two EP combinations it has been found that all possible monic RPs have been generated. The monic RPs have been cancelled out from the list of all monic BPs leaving behind all monic IPs. The monic IPs have been multiplied with all CPs to obtain all non-monic IPs.

In the case of multiplication of two monic EPs, the respective DEs have been split into coefficients of respective EPs. All coefficient of each EP have been multiplied by modulo multiplication with each other along with variables. Next to it the coefficients of the same degree term have been added by modulo addition to obtain the concerned monic BP or monic RP. RPs have been cancelled out from the list of monic BPs to obtain monic IPs.

3.2. Mathematical Method to Search for Monic IPs over Galois Field $GF(7^7)$

Here the interest has been to find the monic IPs over Galois Field or $GF(7^7)$, where $p = 7$ has been the prime field and $q = 7$ has been the extension of that prime field. In general the indices of multiplicand and multiplier have been added to obtain the product. The extension $q = 7$ can be demonstrated as a sum of two integers d_1 and d_2. The degree of the highest degree term present in EPs of $GF(7^7)$ has been $(q - 1) = 6$ through 1. The polynomials with highest degree of term has been 0, are constant polynomials and they do not play any significant role here, so they have been neglected. Hence the two set of monic elemental polynomials for which the product has been a monic BP where $p = 7$, $q = 7$, have the degree of highest degree terms d_1, d_2 where, $d_1 = 1, 2, 3$, and the corresponding values of d_2 are, 6, 5, 4. Here the number of coefficients in the monic basic polynomial, $BP = (q+1) = (7+1) = 8$; they are defined as $BP_0, BP_1, BP_2, BP_3, BP_4, BP_5, BP_6, BP_7$ the value of the suffix also indicates the degree of the term of the monic BP and for monic polynomials $BP_7 = 1$. for this case, total number of blocks is the number of integers in d_1 or d_2, *i.e.* 3.

Coefficients of each term in the 1st monic EP, EP^0 where, $d_1 = 1$; have been defined as EP_0^0, EP_1^0, Coefficients of each term in the 2nd monic EP, EP^1 where $d_2 = 6$; have been defined as $EP_0^1, EP_1^1, EP_2^1, EP_3^1, EP_4^1, EP_5^1, EP_6^1$. The value in

suffix also gives the degree of the term of the monic EPs.

Now, the mathematical method is as follows,

1st block:

$$BP_0 = \left(EP_0^0 \times EP_0^1\right)\%7.$$

$$BP_1 = \left(EP_0^0 \times EP_1^1 + EP_1^0 \times EP_0^1\right)\%7.$$

$$BP_2 = \left(EP_0^0 \times EP_2^1 + EP_1^0 \times EP_1^1\right)\%7.$$

$$BP_3 = \left(EP_0^0 \times EP_3^1 + EP_1^0 \times EP_2^1\right)\%7.$$

$$BP_4 = \left(EP_0^0 \times EP_4^1 + EP_1^0 \times EP_3^1\right)\%7.$$

$$BP_5 = \left(EP_0^0 \times EP_5^1 + EP_1^0 \times EP_4^1\right)\%7.$$

$$BP_6 = \left(EP_0^0 \times EP_6^1 + EP_1^0 \times EP_5^1\right)\%7.$$

$$BP_7 = \left(EP_1^0 \times EP_6^1\right)\%7 = 1.$$

Now the given monic BP is,

$$BP(x) = BP_7x^7 + BP_6x^6 + BP_5x^5 + BP_4x^4 + BP_3x^3 + BP_2x^2 + BP_1x^1 + BP_0x^0.$$

$$D\left(BP(x)\right) = BP_7 7^7 + BP_6 7^6 + BP_5 7^5 + BP_4 7^4 + BP_3 7^3 + BP_2 7^2 + BP_1 7^1 + BP_0 7^0.$$

Coefficients of each term in the 1st monic EP, EP^0 where, $d_1 = 2$; have been defined as EP_0^0, EP_1^0, EP_2^0, Coefficients of each term in the 2nd monic EP, EP^1 where $d_2 = 5$; are defined as $EP_0^1, EP_1^1, EP_2^1, EP_3^1, EP_4^1, EP_5^1$.The value in suffix also gives the degree of the term of the monic EPs.

Now, the mathematical method is as follows,

2nd block:

$$BP_0 = \left(EP_0^0 \times EP_0^1\right)\%7.$$

$$BP_1 = \left(EP_0^0 \times EP_1^1 + EP_1^0 \times EP_0^1\right)\%7.$$

$$BP_2 = \left(EP_0^0 \times EP_2^1 + EP_1^0 \times EP_1^1 + EP_2^0 \times EP_0^1\right)\%7.$$

$$BP_3 = \left(EP_0^0 \times EP_3^1 + EP_1^0 \times EP_2^1 + EP_2^0 \times EP_1^1\right)\%7.$$

$$BP_4 = \left(EP_0^0 \times EP_4^1 + EP_1^0 \times EP_3^1 + EP_2^0 \times EP_2^1\right)\%7.$$

$$BP_5 = \left(EP_0^0 \times EP_5^1 + EP_1^0 \times EP_4^1 + EP_2^0 \times EP_3^1\right)\%7.$$

$$BP_6 = \left(EP_1^0 \times EP_5^1 + EP_2^0 \times EP_4^1\right)\%7.$$

$$BP_7 = \left(EP_1^0 \times EP_5^1\right)\%7 = 1.$$

Now the given monic BP is,

$$BP(x) = BP_7x^7 + BP_6x^6 + BP_5x^5 + BP_4x^4 + BP_3x^3 + BP_2x^2 + BP_1x^1 + BP_0x^0.$$

$$D\left(BP(x)\right) = BP_7 7^7 + BP_6 7^6 + BP_5 7^5 + BP_4 7^4 + BP_3 7^3 + BP_2 7^2 + BP_1 7^1 + BP_0 7^0.$$

Coefficients of each term in the 1st monic EP, EP^0 where, $d_1 = 3$; are defined as $EP_0^0, EP_1^0, EP_2^0, EP_3^0$, Coefficients of each term in the 2nd monic EP, EP^1 where

$d_2 = 4$; are defined as $EP_0^1, EP_1^1, EP_2^1, EP_3^1, EP_4^1$. The value in suffix also gives the degree of the term of the monic EPs.

Now, the mathematical method is as follows,

3rd block:

$$BP_0 = \left(EP_0^0 \times EP_0^1\right)\%7.$$

$$BP_1 = \left(EP_0^0 \times EP_1^1 + EP_1^0 \times EP_0^1\right)\%7.$$

$$BP_2 = \left(EP_0^0 \times EP_2^1 + EP_1^0 \times EP_1^1 + EP_2^0 \times EP_0^1\right)\%7.$$

$$BP_3 = \left(EP_0^0 \times EP_3^1 + EP_1^0 \times EP_2^1 + EP_2^0 \times EP_1^1 + EP_3^0 \times EP_0^1\right)\%7.$$

$$BP_4 = \left(EP_0^0 \times EP_4^1 + EP_1^0 \times EP_3^1 + EP_3^0 \times EP_1^1 + EP_2^0 \times EP_2^1\right)\%7.$$

$$BP_5 = \left(EP_1^0 \times EP_4^1 + EP_2^0 \times EP_3^1 + EP_3^0 \times EP_2^1\right)\%7.$$

$$BP_6 = \left(EP_2^0 \times EP_4^1 + EP_3^0 \times EP_3^1\right)\%7.$$

$$BP_7 = \left(EP_3^0 \times EP_4^1\right)\%7 = 1.$$

Now the given monic BP is,

$$BP(x) = BP_7x^7 + BP_6x^6 + BP_5x^5 + BP_4x^4 + BP_3x^3 + BP_2x^2 + BP_1x^1 + BP_0x^0.$$

$$D\left(BP(x)\right) = BP_7 7^7 + BP_6 7^6 + BP_5 7^5 + BP_4 7^4 + BP_3 7^3 + BP_2 7^2 + BP_1 7^1 + BP_0 7^0.$$

In this way the DEs of all the monic BPs or monic RPs have been pointed out. The monic RPs belonging to the list of monic BPs has been cancelled out leaving behind the monic IPs. Non-monic IPs have been computed with multiplication of a monic IP by α where $\alpha \in GF(p)$ and assumes values from 2 through 6.

3.3. Generalized Mathematical Method to Search for Monic IPs over Galois Field $GF(p^q)$

Here the interest has been to find the monic IPs over Galois Field or $GF(7^7)$, where $p = 7$ has been the prime field and $q = 7$ has been the extension of that prime field. In general the indices of multiplicand and multiplier have been added to obtain the product. The extension q can be demonstrated as a sum of two integers d_1 and d_2. The degree of the highest degree term present in EPs of $GF(p^q)$ has been $(q-1)$ through 1. The polynomials with highest degree of term has been 0, are constant polynomials and they do not play any significant role here, so they have been neglected. Hence the two set of monic elemental polynomials for which the product has been a monic BP, have the degree of highest degree terms d_1, d_2 where, $d_1 = 1, 2, 3, \cdots, (q-1/2)$, and the corresponding values of d_2 have been, $(q-1), (q-2), (q-3), \cdots, q-(q-1/2)$. Here the number of coefficients in the monic basic polynomial, $BP = (q+1)$; they have been defined as $BP_0, BP_1, BP_2, BP_3, BP_4, BP_5, BP_6, BP_7, \cdots, BP_q$, the value of the suffix also indicates the degree of the term of the monic BP and for monic polynomials $BP_7 = 1$. for this case, total number of blocks is the number of integers in d_1 or d_2, *i.e.* $(q$-1/2).

Coefficients of each term in the 1st monic EP, EP^0, where, $d_1 = 1, 2, \cdots, (q-1/2)$; are defined as $EP_0^0, EP_1^0, \cdots, EP_{q-1/2}^0$. Coefficients of each term in the 2nd monic EP, EP^1 where $d_2 = (q-1), (q-2), (q-3), \cdots, q-(q-1/2)$; are defined as $EP_0^1, EP_1^1, EP_2^1, \cdots, EP_{q-(q-1/2)}^1$. The value in suffix also gives the degree of the term of the monic EPs. Total number of blocks is the number of integers in d_1 or d_2, *i.e.* (q-1/2) for this example.

Now, the algebraic method for (q-1/2)th block is as follows,

(q-1/2)th block:

$$BP_0 = \left(EP_0^0 \times EP_0^1\right)\%p.$$

$$BP_1 = \left(EP_0^0 \times EP_1^1 + EP_1^0 \times EP_0^1\right)\%p.$$

$$BP_2 = \left(EP_0^0 \times EP_2^1 + EP_1^0 \times EP_1^1 + EP_2^0 \times EP_0^1\right)\%p.$$

$$BP_3 = \left(EP_0^0 \times EP_3^1 + EP_1^0 \times EP_2^1 + EP_2^0 \times EP_1^1 + EP_3^0 \times EP_0^1\right)\%p.$$

$$\cdots$$

$$BP_{q-1} = \left(EP_0^0 \times EP_{q-1}^1 + EP_1^0 \times EP_{q-2}^1 + \ldots + EP_{q-1/2}^0 \times EP_{(q-1)-q-1/2}^1\right)\%p.$$

$$BP_q = \left(EP_{q-1/2}^0 \times EP_{q-(q-1/2)}^1\right)\%p = 1.$$

Now the given monic BP is,

$$BP(x) = BP_q x^q + BP_{q-1} x^{q-1} + \cdots + BP_4 x^4 + BP_3 x^3 + BP_2 x^2 + BP_1 x^1 + BP_0 x^0.$$

$$D(BP(x)) = BP_q p^q + BP_{q-1} p^{q-1} + \cdots + BP_4 p^4 + BP_3 p^3 + BP_2 p^2 + BP_1 p^1 + BP_0 p^0.$$

Similarly In this way the DEs of all the monic BPs or monic RPs have been pointed out. The monic RPs belonging to the list of monic BPs have been cancelled out leaving behind the monic IPs. Non-monic IPs have been computed with multiplication of a monic IP by α where $\alpha \in GF(p)$ and assumes values from 2 to (p − 1).

3.4. Pseudo Code of the Algorithm of the Proposed Mathematical Method

The pseudo code of the given algorithm has been given as follow,

Prime field: p

Extension of the field: q.

$$d_1 = 1, 2, 3, \cdots, (q/2-1).$$

$$d_2 = (q-1), (q-2), (q-3), \cdots, q-(q/2-1).$$

Number of terms in 1st elemental polynomial: $N(d_1)$.

Number of terms in 1st elemental polynomial: $N(d_2)$.

Number of terms in Basic Polynomial: p.

Coefficients of Basic polynomial = BP_{indx}, where $1 < indx < p$

Coefficients of Elemental polynomials = EP_{indx_i}, where $1 < i < 2$.

Here,

$N(d_1) = N(d_2)$ = Total number of blocks.

Each coefficient of basic polynomial can be derived as follows,

$$BP_{indx} \sum \left(EP_{indx_1}^{p_1} + EP_{indx_2}^{p_2} \right) \% p \tag{i}$$

Where,

$$1 < indx < p, 1 < indx_1 < q - 1/2, (q-1) < indx_2 < q - (q-1)/2$$

$$0 < p_1 < N(d_1) - 1, 0 < p_2 < N(d_2) - 1 \text{ and } indx = indx_1 + indx_2$$

The pseudo code of the $(q - 1/2)^{th}$ block of above mathematical method for Galois Field $GF(p^q)$ has been described as follows, where ep[0] and ep[1] have been the arrays of all possible decimal equivalents of 1st and 2nd monic EPs respectively. EP^0, EP^1 have been the arrays consists of P-nary coefficients of 1st and 2nd monic EPs respectively. *BP* is the array consists of P-nary coefficients of the resultant monic *BP*. Decm_eqv(*BP*(*x*)) is the DE of the resultant monic *BP*.

For(ep[0]=p..$p^{q/2-1}$,ep[1]=p^{q-1}…$p^{q-(q/2-1)}$;ep[0]<2*p..$p^{q/2-1}$,ep[0]<2*p^{q-1}…$p^{q-(q/2-1)}$;ep[0]++,ep[1]++){

for(indx[0] = ep[0];indx[0]<2*ep[0];indx[0]++){

coeff_conv_1st_deg (indx[0],EP^0);

for(indx[1] = ep[1];indx[1]<2*ep[1];indx[1]++){

coeff_conv_2nd_deg (indx[1], EP^1);

$$BP_0 = \left(EP_0^0 \times EP_0^1 \right) \% p;$$

$$BP_1 = \left(EP_0^0 \times EP_1^1 + EP_1^0 \times EP_0^1 \right) \% p;$$

$$BP_2 = \left(EP_0^0 \times EP_2^1 + EP_1^0 \times EP_1^1 + EP_2^0 \times EP_0^1 \right) \% p;$$

$$BP_3 = \left(EP_0^0 \times EP_3^1 + EP_1^0 \times EP_2^1 + EP_2^0 \times EP_1^1 + EP_3^0 \times EP_0^1 \right) \% p;$$

…

$$BP_{q-1} = \left(EP_0^0 \times EP_{q-1}^1 + EP_1^0 \times EP_{q-2}^1 + \cdots + EP_{q/2-1}^0 \times EP_{(q-1)-(q/2-1)}^1 \right) \% p;$$

$$BP_q = \left(EP_{q/2-1}^0 \times EP_{q-(q/2-1)}^1 \right) \% p;$$

$$BP(x) = BP_q x^q + BP_{q-1} x^{q-1} + \cdots + BP_4 x^4 + BP_3 x^3 + BP_2 x^2 + BP_1 x^1 + BP_0 x^0;$$

$$D(BP(x)) = BP_q p^q + BP_{q-1} p^{q-1} + \cdots + BP_4 p^4 + BP_3 p^3 + BP_2 p^2 + BP_1 p^1 + BP_0 p^0;$$

indx[2]++;

End for.

End for.

End for.

3.5. Time Complexity of the Given Pseudo Code

Since the pseudo code of algorithm consists of three nested loops so the time complexity of the algorithm has been $O(n^3)$. The comparison of time complexity of the proposed algorithm with Rabin's and modified rabin's algorithm has been

Table 1. Comparison Table of Proposed Algorithm with other Algos.

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

Table 2. Number of Monic IPs over Given Galois Fields.

Ex.GF.	$GF(3^3)$	$GF(7^3)$	$GF(11^3)$	$GF(101^3)$
Number of monic IPs.	8	112	440	343,400
Ex.GF.	$GF(3^5)$	$GF(7^5)$	$GF(3^7)$	$GF(7^7)$
Number of monic IPs.	50	2157	312	117,648

given below in Table 1.

4. Discussion

From the Experiment on C99 platform the obtained results have been shown in Table 2 given below. The hand on Calculation and analysis of results have been done for $GF(3^3)$, $GF(3^5)$, $GF(3^7)$, $GF(7^3)$, $GF(11^3)$ and it has been proved that the proposed algorithm works correctly on each Galois Fields. From this conclusion, the list of all monic IPs in a monotonically increasing order of DEs has uploaded to links given in ref. [SDS17] and [SDH17]. From the table below and hands on calculation it seems that the calculation is correct and up to date.

From Table 1, it seems that the complexity of other algorithms increases with value of prime p and extension q. But for this algorithm the complexity is same for all p and q. That is why for large value of p and q the algorithm takes few minutes to produce the list of all monic IPs over the examined Galois field. So this algorithm has been proved to be a better algorithm. On the other hand most other algorithms had been developed within concern of binary galois field $GF(2)$ or Galois Field $GF(p)$ where the proposed algorithm is designed in concern of extended Galois field $GF(p^q)$. So the aspects of the proposed algorithm have a broad range of application.

5. 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 mathematical method has been a much simpler method similar to composite polynomial method to find monic IPs over Galois Field $GF(p^q)$. It is able to determine DEs of the monic IPs over Galois Field with a larger value of prime, also with large extensions. So this method can reduce the complexity to find monic IPs over Galois Field $GF(p^q)$ with large value of prime and also with large extensions of the prime field. So this would help the crypto community to build S-boxes or ciphers using IPs over Galois Fields of a large value of prime, also with the large extensions of the prime field.

References

[1] Adams, C. and Tavares, S. (1990) The Structured Design of Cryptographically Good S-Boxes. *Journal of Cryptology*, **3**, 27-41.

[2] Feistel, H. (1971) Block Cipher Cryptographic System. US Patent 3798359.

[3] Data Encryption Standard, Federal Information Processing Standards Publication (FIPS PUB) 46, National Bureau of Standards, Washington, DC (1977).

[4] Data Encryption Standard (DES), Federal Information Processing Standards Publication (FIPS PUB) 46-3, National Institute of Standards and Technology, Gaithersburg, MD (1999).

[5] Daemen, J. and Rijmen, V. (2000) AES Proposal: Rijndael. https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-%20guidelines/documents/aes-development/rijndael-ammended.pdf

[6] Vaudenay, S. and Moriai, S. (1994) Comparison of the Randomness Provided by Some AES Candidates, EUROCRYPT 1994. Springer Verlag, No. 950, 386-397.

[7] https://www.academia.edu/35326794/Title._List_of_DEs_of_All_Monic_IPs_Over_Galois_Field_GF_7_7_

[8] https://www.academia.edu/35326783/Title._List_of_DEs_of_All_Monic_IPs_Over_Galois_Field_GF_101_3_

[9] Church, R. (1935) Tables of Irreducible Polynomials for the First Four Prime Moduli. *Annals of Mathematics*, Second Series, **36**, 198-209. http://www.jstor.org/stable/1968675.

[10] Swan, R.G. (1962) Factorization of Polynomials over Finite Fields. *Pacific Journal of Mathematics*, **12**, 1099-1106. https://projecteuclid.org/euclid.pjm/1103036322.

[11] Bartee, T.C. and Schneider, D.I. (1963) Computation with Finite Fields. *Information and Control*, **6**, 79-98.

[12] Berlekamp, E.R. (1967) Factoring Polynomials over Finite Fields. *Bell System Technical Journal*, **46**, 1853-1859.

[13] Kasami, T., Lin, S. and Peterson, W. (1968) Polynomial Codes. *IEEE Transactions on Information Theory*, **14**, 807-814.

[14] Berlekamp, E.R. (1970) Factoring Polynomials over Large Finite Fields. *Mathematics of Computation*, **24**, 713-735. https://doi.org/10.1090/S0025-5718-1970-0276200-X

[15] Rabin, M.O. (1980) Probabilistic Algorithms in Finite Fields. *SIAM Journal on Computing*, **9**, 273-280. https://doi.org/10.1137/0209024

[16] Lenstra, A.K. (1985) Factoring Multivariate Polynomials over Finite Fields. *Journal of Computer and System Sciences*, **30**, 235-248. https://doi.org/10.1016/0022-0000(85)90016-9

[17] McEliece, R.J. (1987) Factoring Polynomials over Finite Fields. In: McEliece, R.J., Ed., *Finite Fields for Computer Scientists and Engineers*, Springer, Berlin, 75-96.

[18] Rónyai, L. (1988) Factoring Polynomials over Finite Fields. *Journal of Algorithms*, **9**, 391-400. https://doi.org/10.1016/0196-6774(88)90029-6

[19] Wan, D.Q. (1990) Factoring Multivariate Polynomials over Large Finite Fields. *Mathematics of Computation*, **54**, 755-770. https://doi.org/10.1090/S0025-5718-1990-1011448-0

[20] Rybowicz, M. (1990) Search of Primitive Polynomials over Finite Fields. *Journal of Pure and Applied Algebra*, **65**, 139-151. https://doi.org/10.1016/0022-4049(90)90115-X

[21] Shoup, V. (1990) New Algorithms for Finding Irreducible Polynomials over Finite Fields. *Mathematics of Computation*, **54**, 435-447.

[22] Rónyai, L. (1992) Galois Groups and Factoring Polynomials over Finite Fields. *SIAM Journal on Discrete Mathematics*, **5**, 345-365. https://doi.org/10.1137/0405026

[23] Zivkovic, M. (1994) Table of Primitive Binary Polynomials. *Mathematics of Computation*, **63**, 301-306. https://doi.org/10.2307/2153576

[24] Shparlinski, I. (1996) On Finding Primitive Roots in Finite Fields. *Theoretical Computer Science*, **157**, 273-275. https://doi.org/10.1016/0304-3975(95)00164-6

[25] Flajolet, P., Gourdon, X. and Panario, D. (1996) Random Polynomials and Polynomial Factorization. Lecture Notes in Computer Science, Vol. 1099, Springer-Verlag, New York/Berlin, 232-243.

[26] Gao, S. and Panario, D. (1997) Tests and Constructions of Irreducible Polynomials over Finite Fields. In: Cucker, F. and Shub, M., Eds., *Foundations of Computational Mathematics*, Springer, Berlin, Heidelberg, 346-361. https://doi.org/10.1007/978-3-642-60539-0_27

[27] Kaltofen, E. and Shoup, V. (1998) Subquadratic-Time Factoring of Polynomials over Finite Fields. *Mathematics of Computation of the American Mathematical Society*, **67**, 1179-1197. https://doi.org/10.1090/S0025-5718-98-00944-2

[28] Bach, E., von zur Gathen, J. and Lenstra Jr., H.W. (2001) Factoring Polynomials over Special Finite Fields. *Finite Fields and Their Applications*, **7**, 5-28. https://doi.org/10.1006/ffta.2000.0306

[29] Gao, S. and Lauder, A.G.B. (2002) Hensel Lifting and Bivariate Polynomial Factorisation over Finite Fields. *Mathematics of Computation*, **71**, 1663-1676. https://doi.org/10.1090/S0025-5718-01-01393-X

[30] Brent, R.P. and Zimmermann, P. (2003) Algorithms for Finding Almost Irreducible and Almost Primitive Trinomials. In: Van Der Poorten, A., Van Der Poorten, A.J., Stein, A. and Williams, H.C., Eds., *High Primes and Misdemeanours: Lectures in Honour of the* 60*th Birthday of Hugh Cowie Williams*, American Mathematical Society, Providence, 91-102.

[31] Saxena, N.R. and McCluskey, E.J. (2004) Primitive Polynomial Generation Algorithms Implementation and Performance Analysis. Technical Report (CRC TR 04-03), Center for Reliable Computing.

[32] Gao, S., Kaltofen, E. and Lauder, A.G.B. (2004) Deterministic Distinct-Degree Factorization of Polynomials over Finite Fields. *Journal of Symbolic Computation*, **38**, 1461-1470. https://doi.org/10.1016/j.jsc.2004.05.004

[33] Maitraa, S., Gupta, K.C. and Venkateswar, A. (2005) Results on Multiples of Primitive Polynomials and Their Products over GF(2). *Theoretical Computer Science*, **341**, 311-343. https://doi.org/10.1016/j.tcs.2005.04.011

[34] Scott, M. (2007) Optimal Irreducible Polynomials for GF(2m) Arithmetic. Dublin City University, Dublin.

[35] Fernandez, C.K. (2008) Pascal Polynomials over GF(2). Master's Thesis, Naval Postgraduate School Monterey CA Dept. of Mathematics, Accession No. ADA483773.

[36] Saha, C. (2008) A Note on Irreducible Polynomials and Identity Testing.

[37] Ahmed, A. and Lbekkouri, A. (2009) Determination of Irreducible and Primitive Polynomials over a Binary Finite Field. *Conference: Workshop sur les Technologies de l'Information et de la Communication*, Agadir, 24-25 Décembre 2009, 94.

[38] Richards, C. (2009) Algorithms for Factoring Square-Free Polynomials over Finite Fields.

[39] Kim, R. and Koepf, W. (2009) Divisibility of Trinomials by Irreducible Polynomials over F2. *International Journal of Algebra*, **3**, 189-197.

[40] Hanif, S. and Imran, M. (2011) Factorization Algorithms for Polynomials over Finite Fields. Degree Project, School of Computer Science, Physics and Mathematics, Linnaeus University.

[41] Wang, L. and Wang, Q. (2012) On Explicit Factors of Cyclotomic Polynomials over Finite Fields. *Designs, Codes and Cryptography*, **63**, 87-104. https://doi.org/10.1007/s10623-011-9537-6

[42] Couveignes, J.M. and Lercier, R. (2013) Fast Construction of Irreducible Polynomials over Finite Fields. *Israel Journal of Mathematics*, **194**, 77-105. https://doi.org/10.1007/s11856-012-0070-8

[43] Marquis, D. (2014) Deterministic Factorization of Polynomials over Finite Fields. Thesis: MS in Pur Mathematics, Carleton University, Ottawa.

[44] Hammarhjelm, G. (2014) Construction of Irreducible Polynomials over Finite Fields. UUDM Project Report 17, Uppasala Universitet, Uppasala.

[45] Cavanna, N. (2014) Polynomial Factoring Algorithms and Their Computational Complexity. Honors Scholar Theses, 384. http://digitalcommons.uconn.edu/srhonors_theses/384

[46] Wang, J. and Dong, Z. (2014) Simple Method to Find Primitive Polynomials of Degree n over $GF(2)$ Where 2^n-1 Is a Mersenne Prime. http://worldcomp-proceedings.com/proc/p2014/SAM9773.pdf

[47] Sadique Uz Zaman, J.K.M., Dey, S. and Ghosh, R. (2015) An Algorithm to Find the Irreducible Polynomials over Galois Field GF(pm). *International Journal of Computer Applications*, **109**, 24-29.

[48] Ha, J. (2016) Irreducible Polynomials with Several Prescribed Coefficients. *Finite Fields and Their Applications*, **40**, 10-25. https://doi.org/10.1016/j.ffa.2016.02.006

[49] Poonen, B. (2017) Using Zeta Functions to Factor Polynomials over Finite Fields.

[50] Weisstein, E.W. (2004) Integer Polynomial. From MathWorld—A Wolfram Web Resource. http://mathworld.wolfram.com/IntegerPolynomial.html