Multiples of Primitive Polynomials and Their Products over GF(2)

S. Maitra, K. C. Gupta, A. Venkateswarlu
Indian Statistical Institute
203 B T Road, Calcutta 700 108, INDIA
Communicating email : subho@isical.ac.in
*

Abstract

A standard model of nonlinear combiner generator for stream cipher system combines the outputs of several independent Linear Feedback Shift Register (LFSR) sequences using a nonlinear Boolean function to produce the key stream. Given such a model, cryptanalytic attacks have been proposed by finding out the sparse multiples of the connection polynomials corresponding to the LFSRs. In this direction recently a few works are published on t-nomial multiples of primitive polynomials. We here provide further results on degree distribution of the t-nomial multiples. However, finding out the sparse multiples of just a single primitive polynomial does not suffice. The exact cryptanalysis of the nonlinear combiner model depends on finding out sparse multiples of the products of primitive polynomials. We here make a detailed analysis on t-nomial multiples of products of primitive polynomials. We present new enumeration results for these multiples and provide some estimation on their degree distribution.

Keywords : *Primitive Polynomials, Galois Field, Polynomial Multiples, Cryptanalysis, Stream Cipher.*

1 Introduction

Linear Feedback Shift Register (LFSR) is used extensively as pseudorandom bit generator in different cryptographic schemes and the connection polynomials of the LFSRs are the polynomials over GF(2) (see [3, 12, 2] for more details). To get the maximum cycle length these connection polynomials need to be primitive [9]. To resist cryptanalytic attacks, it is important that these primitive polynomials should be of high weight and also they should not have sparse multiples [11, 1] (see also [8] and the references in this paper for current research on cryptanalysis in this direction). With this motivation, finding out sparse multiples of primitive polynomials has received a lot of attention recently, as evident from [6, 4, 5].

[*] This work has been supported by the Rex progam, a joint activity of USENIX Association and Stichting NLnet

It has been reported [5] that given any primitive polynomial of degree d, it has exactly $N_{d,t} = \frac{\binom{2^d-2}{t-2} - N_{d,t-1} - \frac{t-1}{t-2}(2^d-t+1)N_{d,t-2}}{t-1}$ many t-nomial multiples (having constant term 1) with initial conditions $N_{d,2} = N_{d,1} = 0$. In [5], it has been identified that the distribution of the degrees of t-nomial multiples (having constant term 1) of a degree d primitive polynomial $f(x)$ is very close with the distribution of maximum of the tuples having size $(t-1)$ in the range 1 to $2^d - 2$. We here provide further experiments to substantiate this claim. In fact we find that the *square of the degrees of t-nomial multiples* and the *square of the maximum of the tuples having size* $(t-1)$ presents almost similar kind of statistical behaviour. This we discuss in Section 3.

However, in terms of the practical nonlinear combiner model [12, 13], it is important to discuss about the sparse multiples of *products of primitive polynomials* instead of just a single primitive polynomial. In the nonlinear combiner model outputs of several LFSRs are combined using a nonlinear Boolean function. To make such a system safe, it is important to use correlation immune Boolean functions with some important cryptographic properties (see [1] and references in this paper for more details). Even if the combining Boolean function satisfies good cryptographic properties and possesses correlation immunity of order m, it is possible to consider product of $(m+1)$ primitive polynomials for cryptanalysis. Generally the degree of the primitive polynomials are taken to be coprime for generation of key stream having better cryptographic properties [9, Page 224]. Hence, if one can find sparse multiples of the product of primitive polynomials, then it is possible to launch cryptanalytic attacks on the nonlinear combiner model of the stream cipher (see [1] for a concrete description of such an attack).

In this direction we concentrate on t-nomial multiples of products of primitive polynomials. Consider k different primitive polynomials $f_1(x), f_2(x), \ldots, f_k(x)$ having degree $d_1, d_2, \ldots, d_k$ respectively, where $d_1, d_2, \ldots, d_k$ are pairwise coprime. Then the number of t-nomial multiples with degree $< (2^{d_1}-1)(2^{d_2}-1)\ldots(2^{d_k}-1)$ of $f_1(x)f_2(x)\ldots f_k(x)$ is at least $((t-1)!)^{k-1}\prod_{r=1}^{k} N_{d_r,t}$, where $N_{d_r,t}$ is as defined above (see also [5]). In fact, we present a more general result, which works for product of polynomials (may not be primitive) and then as a special case, we deduce the result for products of primitive polynomials. We discuss these issues in Section 4.

In Section 5, we discuss about the degree distribution for t-nomial multiples of product of primitive polynomials having degree pairwise coprime. We try to estimate this distribution and support our claim with experimental results. It is observed that the distribution of the degrees of t-nomial multiples (having constant term 1) of product of primitive polynomials is very close with the distribution of maximum of the tuples having size $(t-1)$. Thus, it is similar to the degree distribution of t-nomial multiples (having constant term 1) of primitive polynomials.

Let us now discuss a few basic concepts in this direction.

2 Preliminaries

The field of 2 elements is denoted by $GF(2)$. $GF(2^d)$ denotes the extension field of dimension d over $GF(2)$. A polynomial is irreducible over a field if it is not the product of two polynomials of lower degree in the field. A primitive polynomial of degree d is an irreducible polynomial if its roots are the generators of the field $GF(2^d)$. The exponent of the polynomial $f(x)$ (having degree $d \geq 1$, with $f(0) = 1$) is $e \leq 2^d - 1$, which is the least positive integer such that $f(x)$ divides $x^e - 1$. For primitive polynomials $e = 2^d - 1$. By a t-nomial we refer to a polynomial with t distinct non zero terms. For more details on finite fields, the reader is referred to [10, 9].

First we revisit some results presented in [5] and show how finding out t-nomial multiples is related to weight enumerator of Hamming codes. This relationship has also been used in [1, Page 580] to estimate the number of parity check equations, but explicit relationship was not investigated.

2.1 Weight enumerator of Hamming code and t-nomial multiples of a primitive polynomial

Consider a primitive polynomial $f(x)$ of degree d and its multiples upto degree $2^d - 2$. This constructs a $[2^d - 1, 2^d - m - 1, 3]$ linear code, which is the well known Hamming code [10]. By $N^*_{d,t}$ we denote the number of codewords of weight (number of 1's in the codeword) t in the Hamming code $[2^d - 1, 2^d - m - 1, 3]$. Now we present the following technical result which connects $N_{d,t}$ and $N^*_{d,t}$.

Theorem 2.1 $N^*_{d,t} = \frac{2^d - 1}{t} N_{d,t}$.

Proof : Consider a primitive polynomial $f(x)$ of degree d over $GF(2)$. Now, $N^*_{d,t}$ is the number of t-nomial multiples with degree $\leq 2^d - 2$ of $f(x)$. Note that, for each of these multiples, the constant term can be either 0 or 1. On the other hand, $N_{d,t}$ is the number of t-nomial multiples having constant term 1 with degree $\leq 2^d - 2$ of $f(x)$.

Let α be a root of $f(x)$. Consider $f(x)$ divides $1 + x^{i_1} + x^{i_2} + \ldots + x^{i_{t-2}} + x^{i_{t-1}}$ for $1 \leq i_1 < i_2 < \ldots < i_{t-2} < i_{t-1} \leq 2^d - 2$. Hence, $1 + \alpha^{i_1} + \alpha^{i_2} + \ldots + \alpha^{i_{t-1}} = 0$. This immediately gives, $\alpha^i(1 + \alpha^{i_1} + \alpha^{i_2} + \ldots + \alpha^{i_{t-1}}) = 0$ for $0 \leq i \leq 2^d - 2$. Thus, there are $(2^d - 1)$ number of distinct t-nomial multiples (having constant term either 0 or 1), corresponding to $1 + x^{i_1} + x^{i_2} + \ldots + x^{i_{t-2}} + x^{i_{t-1}}$. Out of these $(2^d - 1)$ multiples, there are exactly t many multiples having constant term 1. This happens with the original t-nomial and when $i + i_r = 2^d - 1$, for $r = 1, \ldots, t - 1$. Thus, corresponding to each of the $N_{d,t}$ number of multiples *having constant term 1*, we get $\frac{2^d - 1}{t}$ number of distinct t-nomial multiples having constant term either 0 or 1. Hence the result. ■

Some results presented in [5, Section 2] can be achieved using the above theorem.

1. We have $N^*_{d,t} = \frac{\binom{2^d-1}{t-1} - N^*_{d,t-1} - (2^d - t + 1) N^*_{d,t-2}}{t-1}$, from weight enumerator of Hamming code [10, Page 129]. Thus we get $N_{d,t} = \frac{\binom{2^d-2}{t-2} - N_{d,t-1} - \frac{t-1}{t-2}(2^d - t + 1) N_{d,t-2}}{t-1}$ using Theorem 2.1.

2. It is easy to see that $N^*_{d,t} = N^*_{d,2^d-1-t}$. This, using Theorem 2.1 gives, $\frac{N_{d,t}}{t} = \frac{N_{d,2^d-1-t}}{2^d-1-t}$.

3. Consider a t-nomial multiple $1 + x^{i_1} + x^{i_2} + \ldots + x^{i_{t-2}} + x^{i_{t-1}}$ of a primitive polynomial $f(x)$ having degree d. Now, it is clear that $x^i(1 + x^{i_1} + x^{i_2} + \ldots + x^{i_{t-2}} + x^{i_{t-1}})$ gives $2^d - 2 - i_{t-1}$ many t-nomial multiples of $f(x)$ with constant term 0 for $1 \leq i \leq 2^d - 2 - i_{t-1}$. Thus,

each t-nomial multiple, of the form $1 + x^{i_1} + x^{i_2} + \ldots + x^{i_{t-2}} + x^{i_{t-1}}$ counted in $N_{d,t}$ produces one t-nomial multiple (itself) with constant term 1 and $2^d - 2 - i_{t-1}$ many t-nomial multiples with constant term 0. So, $\sum_{r=1}^{N_{d,t}}(2^d - 1 - d_r) = N^*_{d,t}$, where d_r is the degree of t-nomial multiples with constant term 1. This, using Theorem 2.1 gives, $\sum_{r=1}^{N_{d,t}} d_r = \frac{t-1}{t}(2^d - 1)N_{d,t}$.

3 Degree distribution of multiples of primitive polynomials

In [5], the distribution of the degrees for the t-nomial multiples of primitive polynomials has been discussed. We consider the multiples with constant term 1. The importance of the constant term being 1 is as follows. We know from [11] that if the connection polynomial (a primitive one) is of low weight, then it is possible to exploit cryptanalytic attacks. In the same direction, it is also clear that if there is a primitive polynomial $f(x)$ of degree d with high weight which has a t-nomial (t small) multiple $f_t(x)$, then the recurrence relation satisfied by $f(x)$ will also be satisfied by $f_t(x)$. It is then important to find out t-nomial multiples of low degree for fast cryptanalytic attacks. Note that the recurrence relation induced by the t-nomial $1 + x^{i_1} + x^{i_2} + \ldots + x^{i_{t-2}} + x^{i_{t-1}}$ (constant term 1) is same as the recurrence relation induced by any of the t-nomials $x^i(1 + x^{i_1} + x^{i_2} + \ldots + x^{i_{t-2}} + x^{i_{t-1}})$ (constant term may be zero). Thus, it is important to find out distinct t-nomials with constant term 1. This consideration has also been followed in [5].

Given any primitive polynomial $f(x)$ of degree d, it is clear that $f(x)$ has $N_{d,t}$ number of t-nomial multiples having degree $\leq 2^d - 2$. Now it is an important question that how many t-nomial multiples are there having degree less than or equal to some c. Since, this result is not settled, in [5], an estimation has been used. In [5], any t-nomial multiple $1+x^{i_1}+x^{i_2}+\ldots+x^{i_{t-2}}+x^{i_{t-1}}$ has been interpreted as the $(t-1)$-tuple $< i_1, i_2, \ldots, i_{t-2}, i_{t-1} >$. It was also empirically justified using experimental result (considering primitive polynomials of degree 8, 9 and 10, Tables 1, 2, 3 in [5]) that by fixing $f(x)$, if one enumerates all the $N_{d,t}$ different $(t-1)$ tuples, then the distribution of the tuples seems random. Moreover, the distribution of the degrees of the t-nomial multiples seems very close with the distribution of maximum value of each of the ordered tuples $< i_1, i_2, \ldots, i_{t-2}, i_{t-1} >$ with $1 \leq i_1 < i_2 < \ldots < i_{t-2} < i_{t-1} \leq 2^d - 2$.

To analyse the degree distribution of these t-nomial multiples, the random variate X is considered in [5], which is $\max(i_1, i_2, \ldots, i_{t-2}, i_{t-1})$, where $1+x^{i_1}+x^{i_2}+\ldots+x^{i_{t-2}}+x^{i_{t-1}}$ is a t-nomial multiple of $f(x)$. There are $N_{d,t}$ such multiples. The mean value of the distribution of X is $\frac{t-1}{t}(2^d - 1)N_{d,t}$ divided by $N_{d,t}$, i.e., $\overline{X} = \frac{t-1}{t}(2^d - 1)$ (see [5] and Section 2 of this paper). On the other hand, consider all the $(t-1)$-tuples $< i_1, i_2, \ldots, i_{t-2}, i_{t-1} >$ in the range 1 to $2^d - 2$. There are $\binom{2^d-2}{t-1}$ such tuples. Each tuple is in ordered form such that $1 \leq i_1 < i_2 < \ldots < i_{t-2} < i_{t-1} \leq 2^d - 2$. Consider the random variate Y which is $\max(i_1, i_2, \ldots, i_{t-2}, i_{t-1})$. It has been shown in [5] that the mean of this distribution is $\overline{Y} = \frac{t-1}{t}(2^d - 1)$.

Thus, given any primitive polynomial $f(x)$ of degree d, the average degree of its t-nomial multiples with degree $\leq 2^d - 2$ is equal to the average of maximum of all the distinct $(t-1)$ tuples form 1 to $2^d - 2$. With this result and experimental observations, the work of [5] assumes that the distributions X, Y are very close.

3.1 Sum of Squares

We here provide further experimental results in this direction and strengthen the claim of [5] that the distributions X, Y are very close. For this we first find out the sum of squares of $\max(i_1, i_2, \ldots, i_{t-2}, i_{t-1})$ for the distribution Y.

Lemma 3.1 *The average of squares of the values in* Y *is* $\frac{t-1}{t}(2^d-1)(\frac{t2^d}{t+1}-1)$. *Moreover, standard deviation of* Y *is* $\frac{1}{t}\sqrt{\frac{t-1}{t+1}(2^d-1)(2^d-t-1)}$.

Proof : Consider the random variate Y which is $\max(i_1, i_2, \ldots, i_{t-2}, i_{t-1})$. We know that $< i_1, i_2, \ldots, i_{t-2}, i_{t-1} >$ is any ordered $(t-1)$-tuple from the values 1 to 2^d-2. Note that there is only 1 tuple with maximum value $(t-1)$. There are $\binom{t-1}{t-2}$ tuples with maximum value t, $\binom{t}{t-2}$ tuples with maximum value $t+1$ and so on. Thus, the average of the squares of the values in the distribution $Y = \sum_{i=t-1}^{2^d-2} i^2\binom{i-1}{t-2}/\binom{2^d-2}{t-1}$. Now, $\sum_{i=t-1}^{2^d-2} i^2\binom{i-1}{t-2} = (t-1)t\sum_{i=t-1}^{2^d-2}\binom{i+1}{t} - (t-1)\sum_{i=t-1}^{2^d-2}\binom{i}{t-1} = (t-1)t\binom{2^d}{t+1} - (t-1)\binom{2^d-1}{t}$. Simplifying we get, $\sum_{i=t-1}^{2^d-2} i^2\binom{i-1}{t-2}/\binom{2^d-2}{t-1} = \frac{t-1}{t}(2^d-1)(\frac{t2^d}{t+1}-1)$. Now standard deviation of Y $= \sqrt{\frac{t-1}{t}(2^d-1)(\frac{t2^d}{t+1}-1) - (\frac{t-1}{t}(2^d-1))^2} = \frac{1}{t}\sqrt{\frac{t-1}{t+1}(2^d-1)(2^d-t-1)}$. ■

Primitive polynomial	$t = 3$	$t = 4$	$t = 5$	$t = 6$	$t = 7$
x^4+x+1	110	132.61	148.04	158.96	167.13
x^4+x^3+1	110	132.61	148.04	158.96	167.13
Estimated	110	132.75	148	158.92	167.14
x^5+x^2+1	475.33	571.48	636.67	682.78	717.40
x^5+x^3+1	475.33	571.48	636.67	682.78	717.40
$x^5+x^3+x^2+x+1$	475.33	571.48	636.43	682.81	717.44
$x^5+x^4+x^2+x+1$	475.33	571.55	636.41	682.80	717.45
$x^5+x^4+x^3+x+1$	475.33	571.55	636.41	682.80	717.45
$x^5+x^4+x^3+x^2+1$	475.33	571.48	636.43	682.81	717.44
Estimated	475.33	571.95	636.53	682.73	717.42
x^6+x+1	1974	2371.63	2636.76	2827.51	2969.98
$x^6+x^4+x^3+x+1$	1974	2371.09	2636.71	2827.54	2969.99
x^6+x^5+1	1974	2371.63	2636.76	2827.51	2969.98
$x^6+x^5+x^2+x+1$	1974	2371.27	2636.46	2827.54	2970.01
$x^6+x^5+x^3+x^2+1$	1974	2371.09	2636.71	2827.54	2969.99
$x^6+x^5+x^4+x+1$	1974	2371.27	2636.46	2827.54	2970.01
Estimated	1974	2371.95	2637.60	2827.50	2970
x^7+x+1	8043.33	9657.33	10736.02	11505.61	12083.13
x^7+x^3+1	8043.33	9656.92	10736.05	11505.62	12083.13
$x^7+x^3+x^2+x+1$	8043.33	9656.37	10735.46	11505.65	12083.16
x^7+x^4+1	8043.33	9656.92	10736.05	11505.62	12083.13
$x^7+x^4+x^3+x^2+1$	8043.33	9656.65	10735.77	11505.64	12083.14
$x^7+x^5+x^2+x+1$	8043.33	9656.66	10735.87	11505.64	12083.14
$x^7+x^5+x^3+x+1$	8043.33	9657.48	10735.60	11505.61	12083.15
$x^7+x^5+x^4+x^3+1$	8043.33	9656.65	10735.77	11505.64	12083.14
$x^7+x^5+x^4+x^3+x^2+x+1$	8043.33	9657.82	10735.71	11505.60	12083.14
x^7+x^6+1	8043.33	9657.33	10736.02	11505.61	12083.13
$x^7+x^6+x^3+x+1$	8043.33	9656.59	10735.42	11505.65	12083.16
$x^7+x^6+x^4+x+1$	8043.33	9656.59	10735.42	11505.65	12083.16
$x^7+x^6+x^4+x^2+1$	8043.33	9657.48	10735.60	11505.61	12083.15
$x^7+x^6+x^5+x^2+1$	8043.33	9656.66	10735.87	11505.64	12083.14
$x^7+x^6+x^5+x^3+x^2+x+1$	8043.33	9656.38	10735.47	11505.65	12083.16
$x^7+x^6+x^5+x^4+1$	8043.33	9656.37	10735.46	11505.65	12083.16
$x^7+x^6+x^5+x^4+x^2+x+1$	8043.33	9656.38	10735.47	11505.65	12083.16
$x^7+x^6+x^5+x^4+x^3+x^2+1$	8043.33	9657.82	10735.71	11505.60	12083.14
Estimated	8043.33	9658.35	10735.73	11505.60	12083.14

Table 1. Average of *sum of squares for the degrees* of t-nomial multiples. Primitive polynomials with degree 4, 5, 6, 7 are considered.

Here we provide the Table 1 for multiples of primitive polynomials having degree $d = 4, 5, 6, 7$. We take each of the primitive polynomials and then find out the *average of the square of degrees* of t-nomial multiples for $t = 3, 4, 5, 6, 7$. In the last row we present the estimated value $\frac{t-1}{t}(2^d - 1)(\frac{t2^d}{t+1} - 1)$.

From the above table it is clear that in terms of average of squares, the distributions X, Y are very close. The most interesting observation in this direction is the sum of square of the degree of the trinomial multiples. Note that the *average of the squares of the elements of distribution* Y (considering $t = 3$) and *the average of the squares of the degrees of trinomial multiples* are same for all the experiments, which is $\frac{2}{3}(2^d - 1)(3.2^{d-2} - 1)$. Thus we conjecture the following result.

Conjecture 3.1 *Consider any primitive polynomial $f(x)$ of degree d. Consider that the degree of the trinomial multiples (having degree $\leq 2^d - 2$) of $f(x)$ are $d_1, d_2, \ldots, d_{N_{d,3}}$. Then $\sum_{i=1}^{N_{d,3}} d_i^2 = \frac{2}{3}(2^d - 1)(3.2^{d-2} - 1)N_{d,3}$.*

3.2 Reciprocal Polynomials

Consider two primitive polynomials $f(x)$ and $g(x)$ of degree d, such that they are reciprocal to each other. That is, if α is a root of $f(x)$, then $\alpha^{-1} = \alpha^{2^d-2}$ is the root of $g(x)$. Consider the multiset $W(f(x), d, t)$, which contains the degree of all the t-nomial multiples (having degree $< 2^d - 1$) of a degree d polynomial $f(x)$. Now we have the following result.

Lemma 3.2 *Let $f(x)$ and $g(x)$ be two reciprocal primitive polynomials of degree d. Then $W(f(x), d, t) = W(g(x), d, t)$.*

Proof : Note that $f(x)$ divides a t-nomial $x^{i_1} + x^{i_2} + \ldots + x^{i_{t-2}} + x^{i_{t-1}} + 1$ iff $g(x)$ divides a t-nomial $x^{i_1} + x^{i_1-i_2} + \ldots + x^{i_1-i_{t-2}} + x^{i_1-i_{t-1}} + 1$. Without loss of generality, we consider that $i_1 > i_2 > \ldots > i_{t-2} > i_{t-1}$. This gives the proof. ■

From Lemma 3.2 we get that, since $W(f(x), d, t) = W(g(x), d, t)$, the statistical parameters based on $W(f(x), d, t)$ or $W(g(x), d, t)$ are also same. In Table 1, it is clear that the entries corresponding to any primitive polynomial and its reciprocal are same.

4 t-nomial multiples of products of primitive polynomials

We have already mentioned in the introduction that it is important to find out *t-nomial multiples of product of primitive polynomials* instead of *t-nomial multiples of just a single primitive polynomial*. Let us now briefly describe how the exact cryptanalysis works. For more details about the cryptographic properties of the Boolean functions mentioned below, see [1]. Consider $F(X_1, \ldots, X_n)$ is an n-variable, m-resilient Boolean function used in combining the output sequences of n LFSRs S_i having feedback polynomials $c_i(x)$. The Walsh transform of the Boolean function F gives, $W_F(\overline{\omega}) \neq 0$ for some $\overline{\omega}$ with $wt(\overline{\omega}) = m + 1$. This means that the Boolean function F and the linear function $\bigoplus_{i=1}^{n} \omega_i X_i$ are correlated. Let $\omega_{i_1} = \ldots = \omega_{i_{m+1}} = 1$. Now consider the composite LFSR S which produces the same sequence as the XOR of the sequences of the LFSRs $S_{i_1}, \ldots, S_{i_{m+1}}$. The connection polynomial of the composite LFSR will be $\prod_{j=1}^{m+1} c_{i_j}(x)$. Since F and $\bigoplus_{i=1}^{n} \omega_i X_i$ are correlated, the attacks target to estimate the stream generated from the composite LFSR S having the connection polynomial $\psi(x) = \prod_{j=1}^{m+1} c_{i_j}(x)$.

The attack heavily depends on sparse multiples of $\psi(x)$. One such attack, presented in [1], uses t-nomial multiples $t = 3, 4, 5$. In design of this model of stream cipher, generally the degree of the primitive polynomials are taken to be coprime to each other [9, Page 224] to achieve better cryptographic properties. We here take care of that restriction also.

Note that in [1, Page 581], it has been assumed that the approximate count of *multiples of primitive polynomials* and *multiples of products of primitive polynomials* are close. However, this is not always true. In fact, it is possible to find out products of primitive polynomials having same degree which do not have any t-nomial multiple for some t. The construction of BCH code [10] uses this idea. On the other hand, if the degree of the primitive polynomials are pairwise coprime, then we show that it is always guaranteed to get t-nomial multiples of their product provided each primitive polynomial has t-nomial multiples. Moreover, in the next section we will show that the approximate count of *multiples of primitive polynomials* and *multiples of products of primitive polynomials* are close when the degree of the primitive polynomials are mutually coprime (see Remark 5.1). So for this case the assumption of [1, Page 581] is a good approximation. Let us now present the main theorem.

Theorem 4.1 *Consider k many polynomials $f_1(x), f_2(x), \ldots, f_k(x)$ over GF(2) having degrees $d_1, d_2, \ldots, d_k$ and exponents $e_1, e_2, \ldots, e_k$ respectively, with the following conditions :*

1. *$e_1 \neq e_2 \neq \ldots \neq e_k$ are pairwise coprime,*
2. *$f_1(0) = f_2(0) = \ldots = f_k(0) = 1$,*
3. *$gcd(f_r(x), f_s(x)) = 1$ for $1 \leq r \neq s \leq k$,*
4. *number of t-nomial multiples (with degree $< e_r$) of $f_r(x)$ is n_r.*

Then the number of t-nomial multiples with degree $< e_1 e_2 \ldots e_k$ of $f_1(x) f_2(x) \ldots f_k(x)$ is at least $((t-1)!)^{k-1} n_1 n_2 \ldots n_k$.

Proof : Consider that any polynomial $f_r(x)$ has a t-nomial multiple $x^{i_{1,r}} + x^{i_{2,r}} + \ldots + x^{i_{t-1,r}} + 1$ of degree $< e_r$. Now we try to find out a t-nomial multiple of $f_1(x) f_2(x) \ldots f_k(x)$ having degree $< e_1 e_2 \ldots e_k$.

Consider the set of equations $I_1 = i_{1,r} \bmod e_r$ for $r = 1, \ldots, k$. Since $e_1, \ldots, e_k$ are pairwise coprime, we will have a unique solution of $I_1 \bmod e_1 e_2 \ldots e_k$ by Chinese remainder theorem [7, Page 53]. Similarly, consider $I_j = i_{j,r} \bmod e_r$ for $r = 1, \ldots, k$ and $j = 1, \ldots, t-1$. By Chinese remainder theorem, we get a unique solution of $I_j \bmod e_1 e_2 \ldots e_k$.

First we like to show that $f_r(x)$ (for $r = 1, \ldots, k$) divides $x^{I_1} + x^{I_2} + \ldots + x^{I_{t-1}} + 1$. The exponent of $f_r(x)$ is e_r. So we need to show that $f_r(x)$ divides $x^{I_1 \bmod e_r} + x^{I_2 \bmod e_r} + \ldots + x^{I_{t-1} \bmod e_r} + 1$. We have $i_{j,r} = I_j \bmod e_r$ for $r = 1, \ldots, k$, $j = 1, \ldots, t-1$. Thus, $x^{I_1 \bmod e_r} + x^{I_2 \bmod e_r} + \ldots + x^{I_{t-1} \bmod e_r} + 1$ is nothing but $x^{i_{1,r}} + x^{i_{2,r}} + \ldots + x^{i_{t-1,r}} + 1$. Hence $f_r(x)$ (for $r = 1, \ldots, k$) divides $x^{I_1} + x^{I_2} + \ldots + x^{I_{t-1}} + 1$.

Here we need to show that $x^{I_1} + x^{I_2} + \ldots + x^{I_{t-1}} + 1$ is indeed a t-nomial, i.e., $I_j \neq I_l \bmod e_1 \ldots e_k$ for $j \neq l$. If $I_j = I_l$, then it is easy to see that $i_{j,r} = i_{l,r} \bmod e_r$ and hence, $x^{i_{1,r}} + x^{i_{2,r}} + \ldots + x^{i_{t-1,r}} + 1$ itself is not a t-nomial for any r, which is a contradiction.

Moreover, we have $gcd(f_r(x), f_s(x)) = 1$ for $r \neq s$. Thus, $f_1(x)f_2(x)\ldots f_k(x)$ divides $x^{I_1} + x^{I_2} + \ldots + x^{I_{t-1}} + 1$. Also it is clear that degree of $x^{I_1} + x^{I_2} + \ldots + x^{I_{t-1}} + 1$ is less than $e_1e_2\ldots e_k$.

Corresponding to the t-nomial multiple of $f_1(x)$, i.e., $x^{i_{1,1}} + x^{i_{2,1}} + \ldots + x^{i_{t-1,1}} + 1$, we fix the elements in the order $i_{1,1}, i_{2,1}, \ldots, i_{t-1,1}$. Let us name them $p_{1,1}, p_{2,1}, \ldots, p_{t-1,1}$.

For $r = 2, \ldots k$, the case is as follows. Corresponding to the t-nomial multiple $x^{i_{1,r}} + x^{i_{2,r}} + \ldots + x^{i_{t-1,r}} + 1$ of $f_r(x)$, we use any possible permutation of the elements $i_{1,r}, i_{2,r}, \ldots, i_{t-1,r}$ as $p_{1,r}, p_{2,r}, \ldots, p_{t-1,r}$. Thus we will use any of the $(t-1)!$ permutations for each t-nomial multiple of $f_r(x)$ for $r = 2, \ldots, k$.

Now we use Chinese remainder theorem to get I_j having value $< e_1e_2\ldots e_k$ from $p_{j,r}$'s for $r = 1, \ldots, k$. Each $p_{j,r}$ is less than e_r. Note that, $p_{1,r}, p_{2,r}, \ldots, p_{t-1,r}$ (related to $f_r(x)$) can be permuted in $(t-1)!$ ways and we consider the permutation related to all the t-nomials except the first one.

Thus, corresponding to k many t-nomial multiples (one each for $f_1(x), \ldots, f_k(x)$), we get $((t-1)!)^{k-1}$ many t-nomial multiples (degree $< e_1e_2\ldots e_k$) of the product $f_1(x)f_2(x)\ldots f_k(x)$. Using Chinese remainder theorem, it is routine to check that all these $((t-1)!)^{k-1}$ multiples are distinct.

Since, each $f_r(x)$ has n_r distinct t-nomial multiples of degree $< e_r$, the total number of t-nomial multiples of the product $f_1(x)f_2(x)\ldots f_k(x)$ having degree $< e_1e_2\ldots e_k$ is $((t-1)!)^{k-1}n_1n_2\ldots n_k$.

To accept the above count is a lower bound, one needs to show that the t-nomials generated by this method are all distinct. Consider two collections of t-nomial multiples $x^{a_{1,r}} + x^{a_{2,r}} + \ldots + x^{a_{t-1,r}} + 1$ and $x^{b_{1,r}} + x^{b_{2,r}} + \ldots + x^{b_{t-1,r}} + 1$ of $f_r(x)$ for $r = 1, \ldots, k$. There exists at least one s in the range $1, \ldots, k$ such that $x^{a_{1,s}} + x^{a_{2,s}} + \ldots + x^{a_{t-1,s}} + 1$ and $x^{b_{1,s}} + x^{b_{2,s}} + \ldots + x^{b_{t-1,s}} + 1$ are distinct. Let us consider that one of the common multiples form these two sets of t-nomials are same, say $x^{A_{1,v}} + x^{A_{2,v}} + \ldots + x^{A_{t-1,v}} + 1$ (from the set $x^{a_{1,r}} + x^{a_{2,r}} + \ldots + x^{a_{t-1,r}} + 1$) and $x^{B_{1,v}} + x^{B_{2,v}} + \ldots + x^{B_{t-1,v}} + 1$ (from the set $x^{b_{1,r}} + x^{b_{2,r}} + \ldots + x^{b_{t-1,r}} + 1$).

Without loss of generality we consider $A_{1,v} > A_{2,v} > \ldots > A_{t-1,v}$ and $B_{1,v} > B_{2,v} > \ldots > B_{t-1,v}$. Since these two t-nomials are same, we have $A_{j,v} = B_{j,v} \bmod e_1e_2\ldots e_k$. This immediately says that $A_{j,v} = B_{j,v} \bmod e_r$, which implies $a_{j,r} = b_{j,r} \bmod e_r$ for each j in $1, \ldots, t-1$ and each r in $1, \ldots, k$. This contradicts to the statement that $x^{a_{1,s}} + x^{a_{2,s}} + \ldots + x^{a_{t-1,s}} + 1$ and $x^{b_{1,s}} + x^{b_{2,s}} + \ldots + x^{b_{t-1,s}} + 1$ are distinct.

From the above point it is clear that the number of t-nomial multiples with degree $< e_1e_2\ldots e_k$ of $f_1(x)f_2(x)\ldots f_k(x)$ is at least $((t-1)!)^{k-1}n_1n_2\ldots n_k$. ■

Corollary 4.1 *Consider k many primitive polynomials $f_1(x), f_2(x), \ldots, f_k(x)$ having degree $d_1, d_2, \ldots, d_k$ respectively, where $d_1, d_2, \ldots, d_k$ are pairwise coprime. Then the number of t-nomial multiples with degree $< (2^{d_1}-1)(2^{d_2}-1)\ldots(2^{d_k}-1)$ of $f_1(x)f_2(x)\ldots f_k(x)$ is at least $((t-1)!)^{k-1}\prod_{r=1}^{k} N_{d_r,t}$, where $N_{d_r,t}$ is as defined in Theorem 2.1.*

Proof : Since we are considering the primitive polynomials, the exponent $e_r = 2^{d_r} - 1$. Also, given $d_1, d_2, \ldots, d_k$ are mutually coprime, it is clear that $e_1, e_2, \ldots, e_k$ are also mutually coprime. Moreover, There is no common divisor of any two primitive polynomials. The proof then follows from Theorem 4.1 putting $n_r = N_{d_r,t}$. ■

Corollary 4.2 *In Theorem 4.1, for $t = 3$, the number of trinomial multiples with degree $< e_1 e_2 \dots e_k$ of $f_1(x) f_2(x) \dots f_k(x)$ is exactly equal to $2^{k-1} n_1 n_2 \dots n_k$.*

Proof : Consider a trinomial multiple $x^{I_1} + x^{I_2} + 1$ having degree $< e_1 e_2 \dots e_k$ of the product $f_1(x) f_2(x) \dots f_k(x)$. Since, the product $f_1(x) f_2(x) \dots f_k(x)$ divides $x^{I_1} + x^{I_2} + 1$, it is clear that $f_r(x)$ divides $x^{I_1} + x^{I_2} + 1$. Hence, $f_r(x)$ divides $x^{I_1 \bmod e_r} + x^{I_2 \bmod e_r} + 1$ having degree $< e_r$. Now take, $i_{1,r} = I_1 \bmod e_r$ and $i_{2,r} = I_2 \bmod e_r$, for $r = 1, \dots, k$. It is clear that $I_1 \neq I_2 \bmod e_r$ (i.e., $i_{1,r} \neq i_{2,r}$), otherwise $f_r(x)$ divides 1, which is not possible.

Also note that either $i_{1,r}$ or $i_{2,r}$ can not be zero, otherwise $f_r(x)$ divides either $x^{i_{2,r}}$ or $x^{i_{1,r}}$, which is not possible. Thus, $f_r(x)$ divides $x^{i_{1,r}} + x^{i_{2,r}} + 1$. Then using the construction method in the proof of Theorem 4.1, one can get back $x^{I_1} + x^{I_2} + 1$ as the multiple of $f_1(x) f_2(x) \dots f_k(x)$ which is already considered in the count $2^{k-1} n_1 n_2 \dots n_k$ as described in the proof of Theorem 4.1. Hence this count is exact. ■

Corollary 4.3 *Consider k many primitive polynomials $f_1(x), f_2(x), \dots, f_k(x)$ having degree $d_1, d_2, \dots, d_k$ respectively, where $d_1, d_2, \dots, d_k$ are pairwise coprime. Then the number of trinomial multiples with degree $< (2^{d_1} - 1)(2^{d_2} - 1) \dots (2^{d_k} - 1)$ of $f_1(x) f_2(x) \dots f_k(x)$ is exactly equal to $2^{k-1} \prod_{r=1}^{k} N_{d_r,3}$, where $N_{d_r,3}$ is as defined in Theorem 2.1.*

Proof : The proof follows from Corollary 4.1 and Corollary 4.2. ■

In Corollary 4.2 we proved that the number of trinomial multiples of $f_1(x) f_2(x) \dots f_k(x)$ is exactly $2^{k-1} n_1 n_2 \dots n_k$. However, it is important to mention that for $t \geq 4$, $((t-1)!)^{k-1} n_1 n_2 \dots n_k$ is indeed a lower bound and not an exact count. The reason is as follows.

Consider $f_r(x)$ has a multiple $x^{a_{1,r}} + x^{a_{2,r}} + \dots + x^{a_{t-1,r}} + 1$. Note that for $t \geq 5$, we get $(t-2)$-nomial multiples of $f_r(x)$ having degree $< e_r$. Consider the $(t-2)$-nomial multiple as $x^{a_{1,r}} + x^{a_{2,r}} + \dots + x^{a_{t-3,r}} + 1$. Now, from the $(t-2)$-nomial multiple we construct a multiple $x^{a_{1,r}} + x^{a_{2,r}} + \dots + x^{a_{t-1,r}} + 1$, where, $a_{t-2,r} = a_{t-1,r} = w$, where, $w < e_r$. Then if we apply Chinese remainder theorem as in Theorem 4.1, that will very well produce a t-nomial multiple of $f_1(x) f_2(x) \dots f_k(x)$ which is not counted in Theorem 4.1. Thus the count is not exact and only a lower bound. For the case of $t = 4$, we can consider the multiples of the form $x^{i_r} + x^{i_r} + 1 + 1$ of $f_r(x)$. These type of multiples of $f_r(x)$'s will contribute additional multiples of the product $f_1(x) f_2(x) \dots f_k(x)$ which are not counted in Theorem 4.1.

Corollary 4.4 *In Theorem 4.1, for $t \geq 4$, the number of t-nomial multiples with degree $< e_1 e_2 \dots e_k$ of $f_1(x) f_2(x) \dots f_k(x)$ is strictly greater than $((t-1)!)^{k-1} n_1 n_2 \dots n_k$.*

Let us consider the product of two primitive polynomials of degree 3, 4, degree 3, 5 and degree 4, 5 separately. Table 2 compares the lower bound given in Theorem 4.1 and the exact count by running computer program. Note that it is clear that for $t = 3$, the count is exact as mentioned in Corollary 4.3. On the other hand, for $t \geq 4$, the count is a lower bound (strictly greater than the exact count) as mentioned in Corollary 4.4. In Table 2, for a few cases the lower bound is zero, since $N_{3,5} = N_{3,6} = 0$.

t	3	4	5	6	7
Lower bound	42	672	0	0	146160
Exact count	42	1460	35945	717556	11853632

Product of degree 3, 4

t	3	4	5
Lower bound	90	3360	0
Exact count	90	6564	344625

Product of degree 3, 5

t	3	4	5
Lower bound	210	23520	1128960
Exact count	210	32508	3723685

Product of degree 4, 5

Table 2. Count for t-nomial multiples of product of primitive polynomials.

We already know that the lower bound result presented in Corollary 4.1 is invariant on the choice of the primitive polynomials. We observe that this is also true for the exact count found by computer search. As example, if one chooses any primitive polynomial of degree 3 and any one of degree 4, the exact count does not depend on the choice of the primitive polynomials.

Thus we make the following experimental observation. Consider k many primitive polynomials $f_1(x), f_2(x), \ldots, f_k(x)$ having degree $d_1, d_2, \ldots, d_k$ respectively, where $d_1, d_2, \ldots, d_k$ are pairwise coprime. Then the exact number of t-nomial multiples with degree $< (2^{d_1} - 1)(2^{d_2} - 1) \ldots (2^{d_k} - 1)$ of $f_1(x)f_2(x) \ldots f_k(x)$ is same irrespective of the choice of primitive polynomial $f_r(x)$ of degree d_r.

4.1 Exact count vs Lower bound

Note that the values in the Table 2 shows that there are big differences between the exact count and the lower bound. Note that the lower bound in some cases is zero, since $N_{3,5} = N_{3,6} = 0$. We will now clarify these issues.

Let us first present the following result.

Proposition 4.1 *Consider two primitive polynomials $f_1(x), f_2(x)$ of degree d_1, d_2 (mutually coprime) and exponent e_1, e_2 respectively. Then the exact number of 4-nomial multiples of $f_1(x)f_2(x)$ is $6N_{d_1,4}N_{d_2,4} + (e_1 - 1)(e_2 - 1) + (3(e_1 - 1) + 1)N_{d_2,4} + (3(e_2 - 1) + 1)N_{d_1,4}$.*

Proof : The term $6N_{d_1,4}N_{d_2,4}$ follows from Theorem 4.1.

Consider $x^i + x^{k_1e_1} + x^{k_2e_2} + 1$, where $i < e_1e_2$, $i \bmod e_1 \neq 0$, $i \bmod e_2 \neq 0$, and $i = k_2e_2 \bmod e_1 = k_1e_1 \bmod e_2$, $k_1 < e_2$, $k_2 < e_1$. Thus it is clear that for a fixed i, we will get unique k_1, k_2. Now there are $(e_1e_2 - 1) - (e_1 - 1) - (e_2 - 1) = (e_1 - 1)(e_2 - 1)$ possible values of i. Note that in each of the cases, $x^i + x^{k_1e_1} + x^{k_2e_2} + 1$ is divisible by $f_1(x)f_2(x)$. So this will add to the count.

Fix a multiple $x^i + x^j + x^l + 1$ of $f_2(x)$ where i, j, l are unequal and degree of $x^i + x^j + x^l + 1$ is less than e_2. Now consider a multiple $x^a + x^a + x^0 + 1$ of $f_1(x)$. As a varies from 1 to $e_1 - 1$, for each a, we will get three different multiples of $f_1(x)f_2(x)$ by using Chinese remainder theorem. The reason is as follows. Fix the elements $a, a, 0$ in order. Now i, j, k can be placed in $\frac{3!}{2!} = 3$ ways to get distinct cases. Varying a from 1 to $e_1 - 1$, we get $3(e_1 - 1)$ multiples. Moreover, if $a = 0$, then also $x^a + x^a + x^0 + 1$ and $x^i + x^j + x^l + 1$ will provide only one multiple of $f_1(x)f_2(x)$. Thus, considering each multiple of $f_2(x)$ we get $3(e_1 - 1) + 1$ multiples. Hence the total contribution is $(3(e_1 - 1) + 1)N_{d_2,4}$.

Similarly fixing a multiple $x^i + x^j + x^l + 1$ of $f_1(x)$ and $x^a + x^a + x^0 + 1$ of $f_2(x)$ we get the count $(3(e_2 - 1) + 1)N_{d_1,4}$.

It is a routine but tedious exercise to see that all these 4-nomial multiples of $f_1(x)f_2(x)$ are distinct and there is no other 4-nomial multiples having degree $< e_1e_2$. ■

Note that using this formula of Proposition 4.1, we get the exact counts for 4-nomial multiples as presented in Table 2. However, extending the exact formula of 4-nomial multiples of product of two primitive polynomials seems extremely tedious. On the other hand, an important question is *do we at all need the exact count for cryptographic purposes*? We answer this as follows.

Consider that $f_1(x)f_2(x) \ldots f_k(x)$ is itself a τ-nomial with constant term 1. From cryptanalytic point of view, it is interesting to find out t-nomial multiples of $f_1(x)f_2(x) \ldots f_k(x)$

only when $t < \tau$ (in practical cases, $t << \tau$). Now we like to present an interesting experimental observation.

Conjecture 4.1 *Let $x^{I_1} + x^{I_2} + \ldots + x^{I_{t-1}} + 1$ be the least degree t-nomial multiple ($4 \leq t < \tau$) of $f_1(x)f_2(x)\ldots f_k(x)$ which itself is a τ-nomial. Each polynomial $f_r(x)$ is a primitive polynomial of degree d_r (degrees are pairwise coprime) and exponent $e_r = 2^{d_r} - 1$. Moreover, $N_{d_r,t} > 0$. Then $I_v \neq I_w \bmod e_r$ for any $1 \leq v \neq w \leq t-1$ and for any $r = 1, \ldots, k$. That is, the least degree t-nomial multiple of $f_1(x)f_2(x)\ldots f_k(x)$ is the one which is generated as described in Theorem 4.1.*

As example, consider $(x^3+x+1)(x^4+x+1) = x^7+x^5+x^3+x^2+1$ which is itself a 5-nomial. Now the least degree 4-nomial multiple of $x^7 + x^5 + x^3 + x^2 + 1$, as generated in the proof of Theorem 4.1, is $x^9 + x^4 + x^3 + 1$. Note that $x^{9 \bmod 7} + x^{4 \bmod 7} + x^{3 \bmod 7} + 1 = x^2 + x^4 + x^3 + 1$ and $x^{9 \bmod 15} + x^{4 \bmod 15} + x^{3 \bmod 15} + 1 = x^9 + x^4 + x^3 + 1$. Thus the multiple $x^9 + x^4 + x^3 + 1$ is generated as in Theorem 4.1. On the other hand, the least degree 4-nomial multiple of $x^7 + x^5 + x^3 + x^2 + 1$ is $x^{16} + x^{14} + x^9 + 1$, which is not counted in the proof of Theorem 4.1. In this case, $x^{16 \bmod 7} + x^{14 \bmod 7} + x^{9 \bmod 7} + 1 = x^2 + x^0 + x^2 + 1$ (basically 0). This supports the statement of Conjecture 4.1.

We have also checked that the Conjecture 4.1 is true considering products of two primitive polynomials $f_1(x), f_2(x)$ having degree d_1, d_2 (mutually coprime) for $d_1, d_2 \leq 6$.

Remark 4.1 *Let us once again consider the model where outputs of several LFSRs are combined using a nonlinear Boolean function of n variables to produce the key stream. Consider that the combining Boolean function is $(k-1)$th order correlation immune (see [1]). Thus it is possible to mount a correlation attack by considering the product of polynomials $f_r(x), r = 1, \ldots, k$ corresponding to k inputs of the Boolean function. Thus to execute the attack one has to consider the t-nomial multiples of $\prod_{r=1}^{k} f_r(x)$. At this point consider the t-nomial multiples considered in Theorem 4.1. Once we get a t-nomial multiple $x^{I_1} + x^{I_2} + \ldots + x^{I_{t-1}} + 1$ of $\prod_{r=1}^{k} f_r(x)$, we know when we reduce it as $x^{I_1 \bmod e_r} + x^{I_2 \bmod e_r} + \ldots + x^{I_{t-1} \bmod e_r} + 1$, then we will get a t-nomial multiple (having degree $< e_r$) of $f_r(x)$. On the other hand, if we consider any t-nomial multiple $x^{I_1} + x^{I_2} + \ldots + x^{I_{t-1}} + 1$ of $\prod_{r=1}^{k} f_r(x)$, which is not considered in Theorem 4.1, then for some r, $x^{I_1 \bmod e_r} + x^{I_2 \bmod e_r} + \ldots + x^{I_{t-1} \bmod e_r} + 1$, will not be a "genuine" t-nomial multiple (having degree $< e_r$) of $f_r(x)$ (i.e., all the terms will not be distinct). That is we will get either some u such that $I_u = 0 \bmod e_r$ or get some $u \neq v$, such that $I_u = I_v \bmod e_r$. Thus from cryptographic point of view, only the multiples considered in Theorem 4.1 are to be considered.*

5 Degree distribution of t-nomial multiples of product of primitive polynomials

From the cryptanalytic point of view, it is important to find out the t-nomial multiples (of product of primitive polynomials) having lower degrees. One way to obtain the minimum degree t-nomial multiple of product of polynomials is to start checking the t-nomials from lower to higher degrees and see when the first time we get one t-nomial multiple. This provides the minimum degree t-nomial multiple of product of the polynomials. Similar method can be continued further to find out more multiples. On the other hand, to resist cryptanalytic attack, it is important to select primitive polynomials such that they won't have a t-nomial multiple at lower degree for small t, say $t \leq 10$. Thus it is important to analyse the degree distribution of t-nomial multiples of product of primitive polynomials.

Let us now concentrate on the case when the primitive polynomials are of degree pairwise coprime. We like to estimate how the degree of the t-nomial multiples are distributed. Consider a primitive polynomial $f_r(x)$ of degree d_r. It has $N_{d_r,t}$ many t-nomial multiples of degree $< 2^{d_r} - 1$. Now we like to highlight the following points.

1. Consider t-nomial multiples of the form $x^{p_{1,r}} + x^{p_{2,r}} + \ldots + x^{p_{t-1,r}} + 1$ of a primitive polynomial $f_r(x)$. Note that $p_{1,r}, p_{2,r}, \ldots, p_{t-1,r}$ are not ordered and they are distinct mod e_r. Experimental study shows that the values $p_{1,r}, p_{2,r}, \ldots, p_{t-1,r}$ are uniformly distributed in the range $1, 2, \ldots, 2^{d_r} - 2 = e_r - 1$ for each r.

2. Then using Chinese remainder theorem (see the proof of Theorem 4.1), we find out that $f_1(x)f_2(x)\ldots f_k(x)$ divides $x^{I_1} + x^{I_2} + \ldots + x^{I_{t-1}} + 1$ which has degree $< e_1e_2\ldots e_k$. Now in the proof of Theorem 4.1, it is clear that the value I_j is decided from the values $p_{j,r}$'s for $r = 1, \ldots, k$. Since, $p_{j,r}$'s are uniformly distributed and Chinese remainder theorem provides a bijection from $Z_{e_1} \times Z_{e_2} \times \ldots \times Z_{e_k}$ to $Z_{e_1e_2\ldots e_k}$, it is expected that the values $I_1, I_2, \ldots, I_{t-1}$ are uniformly distributed in the range $1, 2, \ldots, e_1e_2\ldots e_k - 1$. Here Z_a is the set of integers from 0 to $a - 1$.

3. The distribution of the degrees of the t-nomial multiples of $f_1(x)f_2(x)\ldots f_k(x)$ is the distribution of $\max(I_1, \ldots, I_{t-1})$. It can be assumed that the values $I_1, I_2, \ldots, I_{t-1}$ are chosen uniformly from the range $1, \ldots, (2^{d_1} - 1)(2^{d_2} - 1)\ldots(2^{d_k} - 1) - 1$.

Product	< 15	< 25	< 35	< 45	< 55	< 65	< 75	< 85	< 95	< 105
10101101	0.0238	0.0714	0.1429	0.1429	0.2619	0.3571	0.5476	0.6429	0.7857	1.0000
11000111	0.0000	0.0476	0.1190	0.1905	0.3095	0.3810	0.5238	0.6190	0.7857	1.0000
11100011	0.0000	0.0476	0.1190	0.1905	0.3095	0.3810	0.5238	0.6190	0.7857	1.0000
10110101	0.0238	0.0714	0.1429	0.1429	0.2619	0.3571	0.5476	0.6429	0.7857	1.0000
$t = 3$	0.0170	0.0515	0.1047	0.1766	0.2672	0.3764	0.5043	0.6509	0.8161	1.0000
10101101	0.0014	0.0110	0.0329	0.0719	0.1349	0.2295	0.3568	0.5253	0.7370	1.0000
11000111	0.0021	0.0103	0.0308	0.0733	0.1349	0.2288	0.3575	0.5247	0.7370	1.0000
11100011	0.0021	0.0103	0.0308	0.0733	0.1349	0.2288	0.3575	0.5247	0.7370	1.0000
10110101	0.0014	0.0110	0.0329	0.0719	0.1349	0.2295	0.3568	0.5253	0.7370	1.0000
$t = 4$	0.0020	0.0111	0.0329	0.0727	0.1362	0.2288	0.3560	0.5232	0.7361	1.0000
10101101	0.0002	0.0021	0.0095	0.0298	0.0689	0.1388	0.2487	0.4196	0.6644	1.0000
11000111	0.0003	0.0024	0.0100	0.0293	0.0677	0.1378	0.2493	0.4204	0.6644	1.0000
11100011	0.0003	0.0024	0.0100	0.0293	0.0677	0.1378	0.2493	0.4204	0.6644	1.0000
10110101	0.0002	0.0021	0.0095	0.0298	0.0689	0.1388	0.2487	0.4196	0.6644	1.0000
$t = 5$	0.0002	0.0023	0.0101	0.0295	0.0688	0.1382	0.2502	0.4196	0.6632	1.0000
10110101	0.0000	0.0005	0.0030	0.0118	0.0345	0.0829	0.1752	0.3356	0.5968	1.0000
11100011	0.0000	0.0005	0.0031	0.0118	0.0345	0.0829	0.1751	0.3356	0.5968	1.0000
11000111	0.0000	0.0005	0.0031	0.0118	0.0345	0.0829	0.1751	0.3356	0.5968	1.0000
10101101	0.0000	0.0005	0.0030	0.0118	0.0345	0.0829	0.1752	0.3356	0.5968	1.0000
$t = 6$	0.0000	0.0005	0.0030	0.0118	0.0344	0.0829	0.1752	0.3357	0.5969	1.0000
11100011	0.0000	0.0001	0.0009	0.0047	0.0171	0.0494	0.1221	0.2679	0.5365	1.0000
10110101	0.0000	0.0001	0.0009	0.0047	0.0170	0.0494	0.1222	0.2679	0.5365	1.0000
11000111	0.0000	0.0001	0.0009	0.0047	0.0171	0.0494	0.1221	0.2679	0.5365	1.0000
10101101	0.0000	0.0001	0.0009	0.0047	0.0170	0.0494	0.1222	0.2679	0.5365	1.0000
$t = 7$	0.0000	0.0001	0.0009	0.0047	0.0170	0.0494	0.1221	0.2679	0.5366	1.0000

Table 3. Degree distribution for t-nomial multiples of product of degree 3 and degree 4 primitive polynomials.

To analyse the degree distribution of these t-nomial multiples of the products of primitive polynomials, let us consider the random variate $X^{(d_1,\ldots,d_k),t}$, which is $\max(I_1, \ldots, I_{t-1})$, where $x^{I_1} + x^{I_2} + \ldots + x^{I_{t-1}} + 1$ is a t-nomial multiple of $f_1(x)f_2(x)\ldots f_k(x)$. Let $\delta = (2^{d_1} - 1)(2^{d_2} - 1)\ldots(2^{d_k} - 1)$. On the other hand, consider all the $(t-1)$-tuples $< I_1, \ldots, I_{t-1} >$, in the *range 1 to $\delta - 1$. There are $\binom{\delta-1}{t-1}$ such tuples. Consider the random variate $Y^{(d_1,\ldots,d_k),t}$, which is* $\max(I_1, \ldots, I_{t-1})$, *where $< I_1, \ldots, I_{t-1} >$ is any ordered t-tuple from the values 1 to $\delta - 1$. With the above explanation and following experimental studies, we consider that the distributions $X^{(d_1,\ldots,d_k),t}$, $Y^{(d_1,\ldots,d_k),t}$ are very close.*

Let us first concentrate on the experimental results presented in Table 3. We consider the degree distribution of t-nomial multiples of product of primitive polynomials of degree 3 and 4. The product polynomials of degree 7 are presented in the leftmost column of the table. As example $(x^3 + x + 1)(x^4 + x + 1) = x^7 + x^5 + x^3 + x^2 + 1$ is represented as 10101101. The exponent of the polynomial $x^7+x^5+x^3+x^2+1$ is $(2^3-1)(2^4-1) = 105$. We present the proportion of t-nomial multiples of degree $< 15, 25, \ldots, 105$, where $t = 3, 4, 5, 6, 7$. Corresponding to each t, we also present the proportion $\binom{c}{t-1}/\binom{\delta-1}{t-1}$ in the last row. Here, $\delta = 105$ and $c = 14, 24, \ldots, 104$. Table 3 clearly identifies the closeness of the distributions $X^{(d_1,\ldots,d_k),t}$, $Y^{(d_1,\ldots,d_k),t}$. Similar support is available from the Table 4 which considers the t-nomial multiples (for $t = 3, 4, 5$) of product of degree 4 and degree 5 primitive polynomials.

Consider two set of primitive polynomials $f_1(x), \ldots, f_k(x)$ and $g_1(x), \ldots, g_k(x)$ of degree $d_1, \ldots, d_k$ (pairwise coprime), such that each $f_r(x)$ and $g_r(x)$ are reciprocal to each other. Consider the multiset $U(f_1(x) \ldots f_k(x), d_1, \ldots, d_k, t)$, which contains the degree of all the t-nomial multiples (having degree $< (2^{d_1} - 1) \ldots (2^{d_k} - 1)$) of $f_1(x) \ldots f_k(x)$. Now we have the following result similar to Lemma 3.2.

Lemma 5.1 $U(f_1(x) \ldots f_k(x), d_1, \ldots, d_k, t) = U(g_1(x) \ldots g_k(x), d_1, \ldots, d_k, t)$.

Since, $U(f_1(x) \ldots f_k(x), d_1, \ldots, d_k, t) = U(g_1(x) \ldots g_k(x), d_1, \ldots, d_k, t)$, the statistical parameters based on $U(f_1(x) \ldots f_k(x), d_1, \ldots, d_k, t)$, and $U(g_1(x) \ldots g_k(x), d_1, \ldots, d_k, t)$ are exactly same. In Table 3, it is clear that the entries corresponding to the multiples $f_1(x)f_2(x)$ and $g_1(x)g_2(x)$ are same where $f_1(x), g_1(x)$ are reciprocal and and $f_2(x), g_2(x)$ are also reciprocal. Thus, in Table 4, we put only one row corresponding to each such pair.

Product	< 30	< 65	< 115	< 165	< 215	< 265	< 315	< 365	< 415	< 465
1101011101	0.0000	0.0286	0.0571	0.1238	0.2095	0.3238	0.4524	0.6095	0.7905	1.0000
1111110001	0.0048	0.0190	0.0619	0.1143	0.2238	0.3238	0.4333	0.6238	0.7952	1.0000
1011111111	0.0000	0.0143	0.0619	0.1333	0.2190	0.3238	0.4619	0.6095	0.7810	1.0000
1001010011	0.0048	0.0190	0.0667	0.1143	0.2190	0.3286	0.4524	0.6286	0.7952	1.0000
1110100111	0.0095	0.0190	0.0571	0.1286	0.2286	0.3238	0.4571	0.6095	0.7952	1.0000
1000000101	0.0095	0.0143	0.0524	0.1286	0.2000	0.3190	0.4571	0.6190	0.7952	1.0000
$t = 3$	0.0040	0.0188	0.0600	0.1244	0.2122	0.3232	0.4575	0.6150	0.7959	1.0000
1101011101	0.0002	0.0023	0.0145	0.0434	0.0969	0.1835	0.3090	0.4819	0.7099	1.0000
1111110001	0.0002	0.0025	0.0142	0.0434	0.0969	0.1834	0.3083	0.4820	0.7099	1.0000
1011111111	0.0002	0.0025	0.0146	0.0433	0.0977	0.1832	0.3091	0.4820	0.7097	1.0000
1001010011	0.0002	0.0023	0.0146	0.0428	0.0973	0.1835	0.3088	0.4820	0.7100	1.0000
1110100111	0.0003	0.0023	0.0145	0.0434	0.0973	0.1830	0.3093	0.4821	0.7099	1.0000
1000000101	0.0004	0.0022	0.0142	0.0433	0.0966	0.1829	0.3086	0.4820	0.7098	1.0000
$t = 4$	0.0002	0.0025	0.0145	0.0436	0.0974	0.1833	0.3089	0.4819	0.7098	1.0000
1101011101	0.0000	0.0003	0.0035	0.0152	0.0446	0.1038	0.2085	0.3774	0.6328	1.0000
1111110001	0.0000	0.0003	0.0035	0.0153	0.0445	0.1037	0.2086	0.3773	0.6328	1.0000
1011111111	0.0000	0.0003	0.0035	0.0152	0.0445	0.1038	0.2084	0.3774	0.6329	1.0000
1001010011	0.0000	0.0003	0.0035	0.0153	0.0445	0.1037	0.2085	0.3773	0.6328	1.0000
1110100111	0.0000	0.0003	0.0035	0.0152	0.0445	0.1037	0.2084	0.3774	0.6328	1.0000
1000000101	0.0000	0.0003	0.0035	0.0152	0.0446	0.1038	0.2084	0.3774	0.6328	1.0000
$t = 5$	0.0000	0.0003	0.0035	0.0152	0.0446	0.1038	0.2084	0.3774	0.6328	1.0000

Table 4. Degree distribution for t-nomial multiples of product of degree 4 and degree 5 primitive polynomials.

Now we present the following result. The proof is similar to the proof of Lemma 3.1.

Lemma 5.2 *Let $\delta = (2^{d_1} - 1)(2^{d_2} - 1) \ldots (2^{d_k} - 1)$. The average of the values in $Y^{(d_1,\ldots,d_k),t}$ is $\frac{t-1}{t}\delta$. Moreover, the average of squares of the values in $Y^{(d_1,\ldots,d_k),t}$ is $\frac{t-1}{t}\delta(\frac{t(\delta+1)}{t+1} - 1)$.*

In the Table 5, we present the exact data for multiples of products of primitive polynomials. We consider the product of primitive polynomials having degree (3, 4), (3, 5) and (4, 5). The product polynomials are presented in the leftmost column of the table. In each cell, we present the experimental values for the distribution $X^{(d_1,d_2),t}$. We present the *average of the degrees* and *average of the squares of the degrees* of t-nomial multiples in the same cell of the table. We also present the estimated values in the tables which gives the results related to the distribution $Y^{(d_1,d_2),t}$. It is clear from the table that for the set of experiments we have done, the results related to the distributions $X^{(d_1,d_2),t}$ and $Y^{(d_1,d_2),t}$ are very close.

Product polynomial	$t = 3$	$t = 4$	$t = 5$
10110101	70.00, 5530.00	78.75, 6595.27	84.00, 7335.44
11100011	70.00, 5530.00	78.75, 6595.15	84.00, 7334.90
Estimated	70.00, 5565.00	78.75, 6678.00	84.00, 7420.00
101000111	144.67, 23580.67	162.75, 28212.40	173.60, 31363.62
100110011	144.67, 23580.67	162.75, 28214.39	173.60, 31362.93
100001001	144.67, 23580.67	162.75, 28213.60	173.60, 31363.82
110101111	144.67, 23580.67	162.75, 28213.88	173.60, 31363.46
111100001	144.67, 23580.67	162.75, 28214.15	173.60, 31362.90
111100001	144.67, 23580.67	162.75, 28216.71	173.60, 31363.33
Estimated	144.67, 23653.00	162.75, 28383.60	173.60, 31537.33
1101011101	310.00, 108190.00	348.75, 129651.90	372.00, 144087.34
1101011101	310.00, 108190.00	348.75, 129659.90	372.00, 144087.41
1101011101	310.00, 108190.00	348.75, 129656.72	372.00, 144086.58
1101011101	310.00, 108190.00	348.75, 129652.81	372.00, 144087.51
1101011101	310.00, 108190.00	348.75, 129652.43	372.00, 144087.20
1101011101	310.00, 108190.00	348.75, 129657.92	372.00, 144087.93
Estimated	310.00, 108345.00	348.75, 130014.00	372.00, 144460.00

Table 5. Average of degree and average of degree square of t-nomial multiples for product of primitive polynomials.

We like to present the following observations from the Table 5, which is related to the distribution $X^{(d_1,\ldots,d_k),t}$.
1. The average of degree of the t-nomial multiples of $\prod_{r=1}^{k} f_r(x)$ is fixed and it is equal to $\frac{t-1}{t}\delta$, where δ is the exponent of $\prod_{r=1}^{k} f_r(x)$.
2. The average of the square of degree of the trinomial multiples of $\prod_{r=1}^{k} f_r(x)$ is fixed but not exactly equal to the estimated value.

From [5, Section 2], we get that it is possible to approximate $N_{d_r,t}$ as $\frac{1}{(t-1)!}2^{d_r(t-2)}$. Now let us concentrate on Corollary 4.4 and for the reason mentioned in Remark 4.1 we are mainly interested in the count $((t-1)!)^{k-1}\prod_{r=1}^{k} N_{d_r,t}$. Thus putting the approximation $N_{d_r,t}$ as $\frac{1}{(t-1)!}2^{d_r(t-2)}$, we get $((t-1)!)^{k-1}\prod_{r=1}^{k} N_{d_r,t} \approx ((t-1)!)^{k-1}\prod_{r=1}^{k}\frac{1}{(t-1)!}2^{d_r(t-2)} = \frac{1}{(t-1)!}2^{(\sum_{r=1}^{k} d_r)(t-2)} = \frac{1}{(t-1)!}2^{d(t-2)}$, where $d = \sum_{r=1}^{k} d_r$, is the degree of $\prod_{r=1}^{k} f_r(x)$.

Remark 5.1 *Consider a primitive polynomial $f(x)$ having degree d and a polynomial $g(x)$, which is product of k different primitive polynomials with degree $d_1, \ldots, d_k$ (pairwise coprime), where $d = d_1 + \ldots + d_k$. From the above discussion, it follows that the approximate count of the t-nomial multiples of $f(x)$ and $g(x)$ are close.*

Consider that we try to find out the lowest degree t-nomial multiple of the product polynomial $\prod_{r=1}^{k} f_r(x)$. Consider this will be of degree c. Thus we expect $(\binom{c}{t-1}/\binom{\delta}{t-1})\prod_{r=1}^{k} N_{d_r,t} \approx 1$, i.e., $(\binom{c}{t-1}/\binom{\delta}{t-1})\frac{1}{(t-1)!}2^{d(t-2)} \approx 1$. Now $\delta = \prod_{r=1}^{k}(2^{d_r}-1) \approx 2^d$. Then we get that $c \approx 2^{\frac{d}{t-1}}$.

Note that the attacks presented by finding out t-nomial multiples of product of primitive polynomials require at least one t-nomial multiple. Consider a scheme using primitive polynomials of degree > 128. If the designer uses an 8-input, 3-resilient Boolean function, then attacker has to consider product of at least 4 primitive polynomials. Thus the degree of the product polynomial will be > 512. In such a scenario, the degree of the lowest degree t-nomial multiple (of the product polynomial) will be approximately as large as $2^{256}, 2^{170}, 2^{128}$ for $t = 3, 4, 5$ respectively. This shows that in such a situation the attacks presented in this direction (see for reference [1]) will not succeed in practical sense. However, for $t = 17$, the approximate degree of the lowest degree t-nomial multiple will be 2^{32}, which is in practical limit. Thus, the work presented in this paper clearly identifies how the parameters should be chosen for safe design of stream cipher systems based on nonlinear combiner model. On the other hand, existing systems can also be revisited to see whether those are still secured given the computational power available now a days and the analysis presented in this paper.

References

[1] A. Canteaut and M. Trabbia. Improved fast correlation attacks using parity-check equations of weight 4 and 5. In *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 573–588. Springer Verlag, 2000.

[2] C. Ding, G. Xiao, and W. Shan. *The Stability Theory of Stream Ciphers.* Number 561 in Lecture Notes in Computer Science. Springer-Verlag, 1991.

[3] S. W. Golomb. *Shift Register Sequences.* Aegean Park Press, 1982.

[4] K. C. Gupta and S. Maitra. Primitive polynomials over GF(2) – A cryptologic approach. In *ICICS 2001*, number 2229 in LNCS, Pages 23–34, November 2001.

[5] K. C. Gupta and S. Maitra. Multiples of primitive polynomials over GF(2). INDOCRYPT 2001, number 2247 in LNCS, Pages 62–72, December 2001.

[6] K. Jambunathan. On choice of connection polynomials for LFSR based stream ciphers. INDOCRYPT 2000, number 1977 in LNCS, Pages 9–18, 2000.

[7] G. A. Jones and J. M. Jones. Elementary Number Theory. Springer Verlag London Limited, 1998.

[8] T. Johansson and F. Jonsson. Fast correlation attacks through reconstruction of linear polynomials. In *Advances in Cryptology - CRYPTO 2000*, number 1880 in Lecture Notes in Computer Science, pages 300–315. Springer Verlag, 2000.

[9] R. Lidl and H. Niederreiter. Introduction to finite fields and their applications. Cambridge University Press, 1994.

[10] F. J. MacWillams and N. J. A. Sloane. *The Theory of Error Correcting Codes.* North Holland, 1977.

[11] W. Meier and O. Stafflebach. Fast correlation attacks on certain stream ciphers. *Journal of Cryptology*, 1:159–176, 1989.

[12] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, September 1984.

[13] T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Transactions on Computers*, C-34(1):81–85, January 1985.