Primitive Polynomials for Robust Scramblers and Stream Ciphers Against Reverse Engineering

Xin-Wen Wu
School of Information and Communication Technology
Griffith University
Gold Coast Campus, QLD 4222, Australia
Email: x.wu@griffith.edu.au

Soo Ngee Koh
School of Electrical and Electronic Engineering
Nanyang Technological University
50 Nanyang Avenue, Singapore 639798
Email: esnkoh@ntu.edu.sg

Chee-Cheon Chui
DSO National Laboratories
20 Science Park Drive
Singapore 118230
Email: ccheeche@dso.org.sg

***Abstract*—A linear feedback shift register (LFSR) is a basic component of a linear scrambler and a stream cipher for a communication system. And primitive polynomials are used as the feedback polynomials of the LFSRs. In a non-cooperative context, the reverse-engineering of a linear scrambler and a stream cipher includes recovering the feedback polynomials and the LFSR's initial states (which are the secret keys in the case of stream ciphers). The problem of recovering the secret keys of stream ciphers has been extensively studied. For example, an effective approach for recovering a secret key is known as the correlation attack in the literature. The problem of reconstructing the feedback polynomials of a stream cipher and a linear scrambler has been studied recently. Both recovering the LFSR initial states by the above-mentioned correlation attack and reconstructing the feedback polynomials are highly dependent on an assumption, that is, they require that the feedback polynomials have sparse multiples of moderate degrees. Hence, in order to build linear scramblers and stream ciphers that are robust against reverse engineering, we should use primitive polynomials which do not have sparse multiples of moderate degrees. In this paper, we study the existence of primitive polynomials which do not have sparse multiples of moderate degrees, and the density of such primitive polynomials among all primitive polynomials. Our results on the existence and density of such primitive polynomials are better than the previous results in the literature.**

I. Introduction

Consider a stream cipher and a linear scrambler of a communication system. A linear feedback shift register (LFSR) is a basic component for both the linear scrambler and stream cipher. In most communication systems, to achieve the maximal period for the sequences produced by the LFSRs, binary primitive polynomials are used as the feedback polynomials of the LFSRs for linear scramblers and stream ciphers. In a non-cooperative context, neither the feedback polynomials nor the initial states of the LFSRs are known by any third party. In the case of stream ciphers, the LFSR initial states are actually the secret keys. Therefore, the reverse-engineering of a linear scrambler and a stream cipher includes recovering the initial states and reconstructing the feedback polynomials.

The problem of recovering the secret keys of stream ciphers has been extensively studied [2], [3], [5], [9], [10], [13] - [19]. For example, one of the effective approaches for recovering a secret key is known as the correlation attack in the literature [2], [14]. The problem of reconstructing the feedback polynomials of a stream cipher has been studied later (see, for example, [1]). Following an idea similar to that of [1], procedures for reconstructing the feedback polynomials of the LFSRs for linear scramblers have been proposed recently [4].

Both recovering the LFSR initial states by the above-mentioned correlation attack and reconstructing the feedback polynomials highly rely on an assumption, that is, they require that the feedback polynomials have sparse multiples of moderate degrees. Hence, in order to build linear scramblers and stream ciphers that are robust against reverse engineering, we should use primitive polynomials which do not have sparse multiples of moderate degrees. Then, a natural and fundamental question is, under what condition, would a primitive polynomial of degree d not have any sparse multiple of a moderate degree? Further, if we randomly take a primitive polynomial of degree d, what is the probability that the primitive polynomial does not have any sparse multiple of a moderate degree? The latter question is equivalent to what is the density of primitive polynomials of degree d which do not have any sparse multiple of a moderate degree among all primitive polynomials of degree d?

Let us first give several definitions, and then precisely describe these questions. In this paper, all polynomials (including primitive polynomials and their multiples) are binary polynomials, i.e., polynomials with coefficients in the binary field $GF(2)$. A polynomial $Q(x)$ is called a multiple of a polynomial $p(x)$, if there exists a polynomial $f(x)$ such that $Q(x) = p(x)f(x)$. In the reverse engineering of scramblers and stream ciphers, only those multiples of primitive polynomials, which contain the constant term 1, are considered. Therefore, in this paper we only consider the multiples $Q(x)$ of primitive polynomials, which have a form $Q(x) = 1 + \sum_{i=1}^{n} c_i x^i$. For any polynomial, $Q(x) = \sum_{i=0}^{n} c_i x^i$ with coefficients $c_0, \ldots, c_n$, the number of nonzero c_i's is called the *number of terms*. If $Q(x)$ has t terms, we call it a *t-nomial*, or a polynomial *of weight t*. A polynomial is called a *sparse polynomial*, if the number of terms of this polynomial is bounded above by a given integer t. The most interesting cases are $t = 3$, 4 or 5 [2]. For a primitive polynomial $p(x)$

of degree d, suppose $Q(x)$ is a multiple of $p(x)$. We say that $Q(x)$ has a *moderate degree*, if the degree of $Q(x)$ is less than or equal to cd^e for a pair of constants c and e, that is, the degree is polynomial but not exponential in d. We are interested in the following two problems:

Problem 1: For given t, c and e, what is the condition on d such that there exists at least one primitive polynomial of degree d, which does not have any multiple of weight at most t and of degree at most cd^e?

Problem 2: For given t, c and e, for a randomly chosen primitive polynomial of degree d, what is the probability that the primitive polynomial does not have any multiple of weight at most t and of degree at most cd^e?

In this paper, we have studied these problems. Note that some results on these problems have been given in [8]. Our results are better than the results in [8], as we will see in Section 5.

The paper is organized as follows. In Section 3, we summarize the existing results related to Problems 1 and 2. The main results on the existence and density of primitive polynomials which do not have any sparse multiple of moderate degree are given in Sections 3 and 4, respectively. In Section 5, we compare our results with the existing results. We conclude the paper by Section 6.

II. Related work

It is well known that any binary primitive polynomial $p(x)$ of degree d divides $x^{2^d-1}-1$. And $n=2^d-1$ is the smallest positive integer such that $p(x)$ divides x^n-1 and x^n+1 (note that $x^n+1=x^n-1$ as binary polynomials). As a result, we do not consider binomial multiples for Problems 1 and 2. Regarding trinomial multiples, some results have been given in [6], [8]. We summarize the results in these papers as follows.

Proposition 2.1: ([6], [8]) Let $p(x)$ be a primitive polynomial of degree d. Then

(1) There exists a trinomial multiple of $p(x)$, with degree less than 2^d-1.

(2) $p(x)$ has exactly $(2^{d-1}-1)$ distinct trinomial multiples of degree less than 2^d-1.

(3) Suppose D is the minimal degree of trinomial multiples of $p(x)$. Then

$$D \le \frac{2^d+2}{3}.$$

(4) If d is an even number, then $x^{\frac{2}{3}(2^d-1)}+x^{\frac{1}{3}(2^d-1)}+1$ is a trinomial multiple of $p(x)$.

For more results on the multiples of a primitive polynomial, see [6], [7], [8], [12]. However, these results do not answer Problems 1 and 2 directly, as we are interested in the multiples with moderate degree (that is, with degree $\le cd^e$ which is polynomial but not exponential in d).

In [8] the author gave the following results. Though they presented some answers to Problems 1 and 2, in Section 5 we will show that our results are better than these results.

Proposition 2.2: ([8]) For a given $t \ge 2$ and $e \ge 1$, if d is such that $1.548^d - 1 \ge (t-1)\binom{d^e+1}{t}$ then there exists at least one primitive polynomial of degree d which does not have any t-nomial multiple of degree $\le d^e$.

Proposition 2.3: ([8]) Given $t \ge 2$ and $e \ge 1$, if d is such that $\phi(2^d-1) > (t-1)\binom{d^e+1}{t}$ then the probability that a randomly chosen primitive polynomial of degree d does not have any t-nomial multiple of degree $\le d^e$ is $\ge 1 - \frac{(t-1)\binom{d^e+1}{t}}{\phi(2^d-1)}$.

III. Existence of good primitive polynomials

In this section, we study Problem 1. For convenience, we call a primitive polynomial of degree d, which does not have any multiple of weight at most t and of degree at most cd^e, a *good primitive polynomial*.

We start with counting the number of binary primitive polynomials. Denote by N_d the number of binary primitive polynomials of degree d; and denote by $\phi()$ the Euler's totient function. It is well known that the number of binary primitive polynomials of degree d is given as

$$N_d = \frac{\phi(2^d-1)}{d}.$$

Regarding the Euler's totient function, the following are well-known properties in the literature.

(P1) When n is a composite, $\phi(n) \le n - \sqrt{n}$.

(P2) When n is a prime, $\phi(n) = n-1$.

(P3) For any integer greater than 1, we have $\phi(n) \ge \sqrt{n}$.

Instead of directly counting (or estimating) the number of primitive polynomials of degree d which do not have any multiple of weight at most t and of degree at most cd^e, we first give an estimate of the number of primitive polynomials which have multiples of weight at most t and of degree at most D. For $D \le 2^d-2$ and $t \ge 3$, we denote by $N_{(d;\,t,D)}$ the number of primitive polynomials of degree d, which have a t-nomial multiple of degree at most D; and denote by $N_{(d;\,\le t,D)}$ the number of primitive polynomials of degree d, which have a multiple of weight at most t and of degree at most D. The following is a key result of this paper.

Theorem 3.1: The number of primitive polynomials of degree d, which have a t-nomial multiple of degree at most D, is bounded from above by

$$N_{(d;\,t,D)} \le \sum_{i=d}^{D} \left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{t-2},$$

where $\lfloor x \rfloor$ is the greatest integer smaller than or equal to x. And the number of primitive polynomials of degree d, which have a multiple of weight at most t and of degree at most D, is bounded from above by

$$N_{(d;\,\le t,D)} \le \sum_{i=d}^{D} \sum_{j=3}^{t} \left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{j-2}.$$

Proof: For a polynomial to be a multiple of a polynomial of degree d, it should have a degree greater than or equal to d. We first count the number of j-nomial polynomials (which contain the constant term 1) of degree i for $i \geq d$, which is

$$\binom{i-1}{j-2}.$$

Now, for any polynomial of degree i, it has at most $\lfloor \frac{i}{d} \rfloor$ factors of degree d. Thus, the number of binary polynomials of degree d, which have a t-nomial multiple (that contains the constant term 1) of degree i, is bounded from above by

$$\left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{t-2}.$$

Therefore, the number of binary primitive polynomials of degree d, which have a t-nomial multiple (that contains the constant term 1) of degree at most D, satisfies

$$N_{(d;\, t,D)} \leq \sum_{i=d}^{D} \left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{t-2}.$$

The second bound can be proved in a similar way. □

We are now ready to give a general condition on d such that there exists at least one good primitive polynomial of degree d.

Theorem 3.2: For any d satisfying

$$\phi(2^d-1) > \sum_{i=d}^{cd^e} d \left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{t-2}$$

there exists at least one binary primitive polynomial of degree d, which does not have any t-nomial multiple of degree $\leq cd^e$.

Proof: There exists at least one binary primitive polynomial of degree d which does not have any t-nomial multiple of degree $\leq cd^e$, if the number of binary primitive polynomials of degree d is strictly greater than the number of binary primitive polynomials of degree d which have a t-nomial multiple of degree at most cd^e. By Theorem 3.1, this is guaranteed by $\phi(2^d-1) > \sum_{i=d}^{cd^e} d \left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{t-2}$. □

Similarly we have the following result.

Theorem 3.3: For any d satisfying

$$\phi(2^d-1) > \sum_{i=d}^{cd^e} \sum_{j=3}^{t} d \left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{j-2}$$

there exists at least one binary primitive polynomial of degree d, which does not have any multiple of weight at most t and of degree $\leq cd^e$.

Remark 3.1: Let us analyze the results given in Theorems 3.2 and 3.3. By the Property (P3) of the Euler's totient function, $\phi(2^d-1) \geq \sqrt{2^d-1}$. It is clear that $\sqrt{2^d-1}$ is an exponential function in d, while both $\sum_{i=d}^{cd^e} d \left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{t-2}$ and $\sum_{i=d}^{cd^e} \sum_{j=3}^{t} d \left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{j-2}$ are polynomial functions in d. Therefore, when d is greater than *some value*, it is always true that $\phi(2^d-1) > \sum_{i=d}^{cd^e} d \left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{t-2}$ and $\phi(2^d-1) > \sum_{i=d}^{cd^e} \sum_{j=3}^{t} d \left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{j-2}$. This means that when d is greater than *some value*, we always have primitive polynomials of degree d, which do not have any sparse multiple of a moderate degree. Later, we will find out these interesting values for the most important cases, that is, the cases of $3 \leq t \leq 5$, $c = 1$ and $e = 2$.

Moreover, the number of binary primitive polynomials $\frac{\phi(2^d-1)}{d}$, which is an exponential function in d, is much greater than the polynomial functions in d, namely $\sum_{i=d}^{cd^e} \left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{t-2}$ and $\sum_{i=d}^{cd^e} \sum_{j=3}^{t} \left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{j-2}$, when d is large enough. This implies that for large d, most of the primitive polynomials are good primitive polynomials. In the next section, we give two lower bounds on the probability of a randomly chosen primitive polynomial to be a good primitive polynomial. □

Corollary 3.4: Consider multiples of weight 3 or 4.

(1) For any d satisfying $d \geq 29$, there always exist binary primitive polynomials of degree d, which do not have any tri-nomial multiples of degree $\leq d^2$.

(2) For any d satisfying $d \geq 41$, there always exist binary primitive polynomials of degree d, which do not have any 4-nomial multiples of degree $\leq d^2$.

Corollary 3.5: For any d satisfying $d \geq 53$, there always exist binary primitive polynomials of degree d, which do not have any multiple of weight ≤ 5 and of degree $\leq d^2$.

IV. Density of good primitive polynomials

Denote by $\widetilde{N}_{(d;t,cd^e)}$, the number of primitive polynomials of degree d, which do not have any t-nomial multiples of degree at most cd^e; and denote by $\widetilde{N}_{(d;\leq t,cd^e)}$, the number of primitive polynomials of degree d, which do not have any multiples of weight at most t and of degree at most cd^e. Then, the *density* of primitive polynomials of degree d which do not have any t-nomial multiple of degree $\leq cd^e$, among all primitive polynomials of degree d, is defined as the ratio $\frac{\widetilde{N}_{(d;t,cd^e)}}{N_d}$. The *density* of primitive polynomials of degree d which do not have any multiple of weight at most t and of degree $\leq cd^e$, among all primitive polynomials of degree d, is defined as $\frac{\widetilde{N}_{(d;\leq t,cd^e)}}{N_d}$. It is clear that Problem 2 proposed in the introductory section is equivalent to the following problem: what is the density of good primitive polynomials?

From the definitions, we have $\widetilde{N}_{(d;t,cd^e)} = N_d - N_{(d;t,cd^e)}$ and $\widetilde{N}_{(d;\leq t,cd^e)} = N_d - N_{(d;\leq t,cd^e)}$, where $N_d = \frac{\phi(2^d-1)}{d}$ is the number of primitive polynomials of degree d. By Theorem 3.1, we have the following results.

Theorem 4.1: The density of of primitive polynomials of degree d which do not have any t-nomial multiple of degree

$\leq cd^e$, among all primitive polynomials of degree d, satisfies

$$\frac{\widetilde{N}_{(d;t,cd^e)}}{N_d} \geq 1 - \frac{\sum_{i=d}^{cd^e} d \cdot \lfloor \frac{i}{d} \rfloor \binom{i-1}{t-2}}{\phi(2^d-1)}.$$

The density of primitive polynomials of degree d which do not have any multiple of weight at most t and of degree $\leq cd^e$, among all primitive polynomials of degree d, satisfies

$$\frac{\widetilde{N}_{(d;\leq t,cd^e)}}{N_d} \geq 1 - \frac{\sum_{i=d}^{cd^e} \sum_{j=3}^{t} d \cdot \lfloor \frac{i}{d} \rfloor \binom{i-1}{j-2}}{\phi(2^d-1)}.$$

From this theorem, for any given d we can easily estimate the density of good primitive polynomials. As an example, from Theorem 4.1 surprisingly we get the following result, which implies that almost all the primitive polynomials of degree $d \geq 75$ do not have any multiple of weight ≤ 5 and of degree $\leq d^2$.

Corollary 4.2: When $d \geq 75$, more than 99.9999% of the primitive polynomials of degree d do not have any multiple of weight ≤ 5 and of degree $\leq d^2$.

Let us see more numerical results. In the following figures (namely, Figures 1 and 2) we show the density of primitive polynomials which do not have any multiple of weight ≤ 5 and of degree $\leq d^2$. In the figures, the horizontal axes represent the degree d of the primitive polynomials; the vertical axes represent the density. The curves represent the values of the lower bound $1 - \frac{\sum_{i=d}^{cd^e} \sum_{j=3}^{t} d \cdot \lfloor \frac{i}{d} \rfloor \binom{i-1}{j-2}}{\phi(2^d-1)}$ of the density given by Theorem 4.1.

From Figure 1 we see that when $d \geq 57$, more than 90% of the primitive polynomials of degree d do not have any multiple of weight ≤ 5 and of degree $\leq d^2$. When $d \geq 70$ the percentage of such good primitive polynomials is approaching 100%.

In Figure 2, we have a closer look at the case of degree $d \geq 70$. And we can see that when $d \geq 71$, more that 99.99% primitive polynomials of degree d do not have any multiple of weight ≤ 5 and of degree $\leq d^2$.

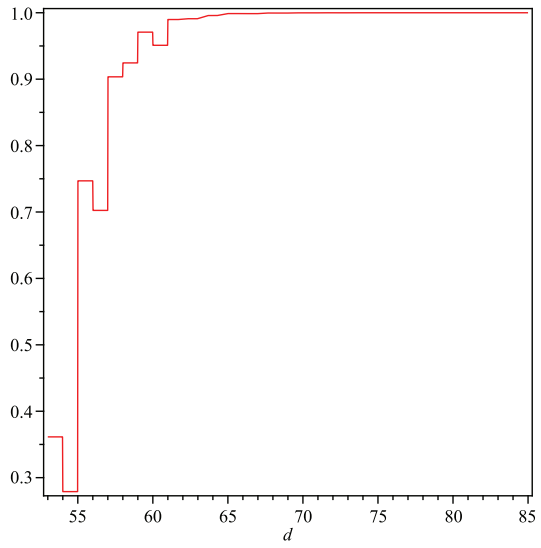

Fig. 1. Density of good primitive polynomials of degree ≥ 53

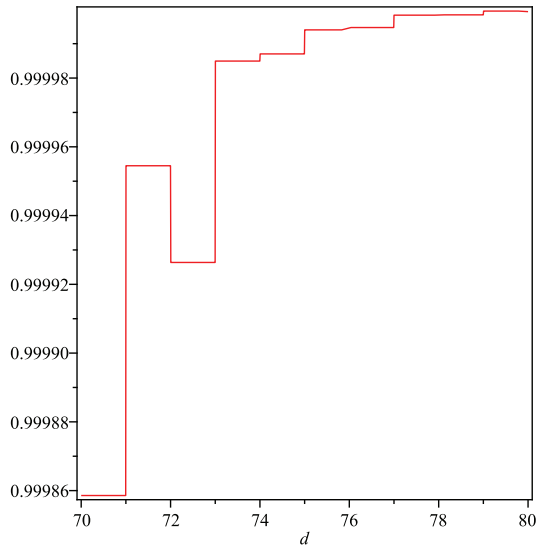

Fig. 2. Density of good primitive polynomials of degree ≥ 70

V. Comparison of our results with previous results

In paper [8], the author studied the existence of primitive polynomials of degree d, which do not have any t-nomial multiple of degree $\leq d^e$. It was showed that (see Theorem 5 of [8], or Proposition 2.2 of this paper) when

$$1.548^d - 1 \geq (t-1)\binom{d^e+1}{t}$$

there exists at least one primitive polynomial of degree d which does not have any t-nomial multiple of degree $\leq d^e$.

Let us compare our result in Theorem 3.2 with the result in [8]. Denote by $\delta_{(t,e)}$ a lower bound such that when $d \geq \delta_{(t,e)}$, there exists at least one primitive polynomial of degree d which does not have any t-nomial multiple of degree $\leq d^e$. From Theorem 3.2 and [8], we can compute two values of $\delta_{(t,e)}$, respectively, for any given pair (t,e).

In the following table, we include the values of $\delta_{(t,e)}$ for the cases of $e = 2, 3, 4$, and $t = 3, 4, 5$. In the table, the rows 2-4 are for $e = 2$ and $t = 3, 4, 5$, respectively. The rows 5-7 are for $e = 3$. And the rows 8-10 are for $e = 4$. The second column shows the results from [8]. And the third column shows the results from our Theorem 3.2. It is clear that for any given (t,e), our value of $\delta_{(t,e)}$ is much smaller than that of [8].

In Table 1, our results show that it is not necessary to have $d \geq 52$ to find good primitive polynomials. In fact, one can

	The results in [8]	Our results
$t=3$	$\delta_{(3,2)}=52$	$\delta_{(3,2)}=29$
$t=4$	$\delta_{(4,2)}=75$	$\delta_{(4,2)}=41$
$t=5$	$\delta_{(5,2)}=97$	$\delta_{(3,2)}=53$
$t=3$	$\delta_{(3,3)}=91$	$\delta_{(3,3)}=49$
$t=4$	$\delta_{(4,3)}=129$	$\delta_{(4,3)}=73$
$t=5$	$\delta_{(5,3)}=169$	$\delta_{(5,3)}=95$
$t=3$	$\delta_{(3,4)}=132$	$\delta_{(3,4)}=73$
$t=4$	$\delta_{(4,4)}=187$	$\delta_{(4,4)}=107$
$t=5$	$\delta_{(5,4)}=244$	$\delta_{(5,4)}=139$

TABLE I
COMPARISON OF OUR RESULTS WITH THE RESULTS IN [8]

find good primitive polynomials for smaller d, which translates to lower implementation complexity. Obviously, the smaller the value of $\delta_{(t,\,e)}$, the better the result.

In [8] the author claimed that it could be proved that for d satisfying $\phi(2^d-1) > (t-1)\binom{d^e+1}{t}$, there exists at least one primitive polynomial of degree d which does not have any t-nomial multiple of degree $\leq d^e$. However, our result in Theorem 3.2 is still better than this result in [8]. In fact, it is easy to prove that $(t-1)\binom{d^e+1}{t} > \sum_{i=d}^{d^e} d\left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{t-2}$. Thus, any d such that $\phi(2^d-1) > (t-1)\binom{d^e+1}{t}$ must satisfy $\phi(2^d-1) > \sum_{i=d}^{d^e} d\left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{t-2}$. Hence, our lower bound $\delta_{(t,e)}$ is still smaller than that of [8].

Theorem 3.3 gave a condition on d such that there exists at least one good primitive polynomial of degree d.

Obviously, this result is independent of Theorem 3.2. For example, from Theorem 3.2 we have proved that when $d \geq 41$, there exists at least one primitive polynomials which does not have any 4-nomial multiple of degree $\leq d^2$. However, $d \geq 41$ will not guarantee that there exists at least one primitive polynomials which does not have any multiple of weight at most 4 and of degree $\leq d^2$.

Next, let us compare our results on density of good primitive polynomials, i.e., Theorem 4.1, with the results in [8]. As mentioned above, $(t-1)\binom{d^e+1}{t} > \sum_{i=d}^{d^e} d\left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{t-2}$, which implies that

$$1 - \frac{\sum_{i=d}^{d^e} d\left\lfloor \frac{i}{d} \right\rfloor \binom{i-1}{t-2}}{\phi(2^d-1)} \geq 1 - \frac{(t-1)\binom{d^e+1}{t}}{\phi(2^d-1)}.$$

Therefore, our results in Theorem 4.1 are better than the results in [8].

VI. CONCLUSION

It is known that linear scramblers and stream ciphers are more vulnerable to reverse engineering if their LFSRs have sparse multiples of moderate degree. Hence, in order to improve the security of a digital communication system, we should use primitive polynomials that do not have any sparse multiple of moderate degree as the feedback polynomials. In this paper, we have studied the conditions on the existence of such primitive polynomials, as well as the probability that a randomly chosen primitive polynomial does not have any sparse multiple of moderate degree. We compared our results with previous results, and our results show that there exist good primitive polynomials of smaller degree d and are better than the existing results.

ACKNOWLEDGMENT

Part of the work of Xin-Wen Wu has been done with the University of Ballarat.

REFERENCES

[1] A. Canteaut and E. Filiol, "Ciphertext only reconstruction of stream ciphers based on combination generators," *Proc. Seventh Intl Workshop Fast Software Encryption (FSE 00)*, pp. 165-180, 2000.

[2] A. Canteaut and M. Trabbia, "Improved fast correlation attacks using parity-check equations of weight 4 and 5," *Proc. Intl Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT 00)*, pp. 573-588, 2000.

[3] V. Chepyzhov and B. Smeets, "On a fast correlation attack on certain stream ciphers," In *Advances in Cryptology - EUROCRYPT'91*, Lecture Notes in Computer Science, vol.547, pp.176-185, Springer-Verlag, 1991.

[4] M. Cluzeau, "Reconstruction of a linear scrambler," *IEEE Trans. Computers*, vol.56, no.9. pp.1283-1291, 2007.

[5] M.P.C. Fossorier, M.J. Mihaljević, and H. Imai, "Modeling block decoding approaches for the fast correlation attack," *IEEE Trans. Inform. Theory*, vol.53, no.12, pp.4728-4737, 2007.

[6] K. Gupta and S. Maitra, "Primitive polynomials over GF(2) - a cryptologic approach," *Lecture Notes in Computer Science*, 2229, Springer-Verlag, pp.23-34, 2001.

[7] K. Gupta and S. Maitra, "Multiples of primitive polynomials over GF(2)," *Lecture Notes in Computer Science*, 2247, Springer-Verlag, pp.62-72, 2001.

[8] K. Jambunathan, "On choice of connection-polynomials for LFSR-based stream ciphers," *Lecture Notes in Computer Science*, Springer-Verlag, pp.9-18, 2000.

[9] T. Johansson and F. Jönsson, "Improved fast correlation attack on stream ciphers via convolutional codes," In: *Advances in Cryptology - EUROCRYPT'99*, Lecture Notes in Computer Science, no. 1592, pp.347-362, Springer-Verlag, 1999.

[10] T. Johansson and F. Jönsson, "Fast correlation attack based on turbo code techniques," In: *Advances in Cryptology - CRYPTO'99*, Lecture Notes in Computer Science, no. 1666, pp.181-197, Springer-Verlag, 1999.

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

[12] S. Maitra, K. Gupta, and A. Venkateswarlu, "Multiples of primitive polynomials and their products over GF(2)," *Lecture Notes in Computer Science*, 2595, Springer-Verlag, pp.214-231, 2003.

[13] W. Meier and O. Staffelbach, "Fast correlation attack on stream ciphers," In: *Advances in Cryptology - EUROCRYPT'88*, Lecture Notes in Computer Science, vol.330, pp. 301-314, Springer-Verlag, 1988.

[14] W. Meier and O. Staffelbach, "Fast correlation attack on certain stream ciphers," *J. Cryptology*, vol. 1, no. 3, pp. 159-176, 1989.

[15] W.T. Penzhorn, "Correlation attacks on stream ciphers: computing low-weight parity check based on error-correcting codes," In: *Fast Software Encryption 96*, Lecture Notes in Computer Science, vol. 1039, pp.159-172, Springer-Verlag, 1996.

[16] W.T. Penzhorn and G.J. Kühn, "Computation of low-weight parity checks for correlation attacks on stream ciphers," In: *Cryptography and Coding -5th IMA Conference*, Lecture Notes in Computer Science, vol. 1025, pp. 74-83, Springer-Verlag, 1995.

[17] R.A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, 1986.

[18] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inform. Theory*, vol. 30, no. 5, pp.776-780, 1984.

[19] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," *IEEE Trans. Computers*, vol. 34, no. 1, pp.81-84, 1985.