PERGAMON Computers and Mathematics with Applications 39 (2000) 31–38

An International Journal
computers & mathematics
with applications

www.elsevier.nl/locate/camwa

# New Upper Bounds on the Linear Complexity

P. CABALLERO-GIL
DEIOC, Universidad de La Laguna
38271 La Laguna, Tenerife, Spain
pcaballe@ull.es.

*(Received and accepted August 1999)*

**Abstract**—In this work, the general upper bound on the linear complexity given by Key is improved for certain families of nonlinear filter functions. Also, a new class of cyclotomic cosets whose degeneration is relatively easy to prove in several conditions is introduced and analysed. 

**Keywords**—Linear complexity, Nonlinear filter function, Cyclotomic coset, Key stream generator, Cryptography.

## 1. INTRODUCTION

A common type of keystream generator, the so-called nonlinear filter generator, consists of a nonlinear function applied to the stages of a linear feedback shift register (LFSR) of length $L$. To provide secure encryption, the key stream must be unpredictable. The linear complexity of a sequence is defined as the length of the shortest linear feedback shift register that can be used to generate it. Since some algorithms make it possible to determine the linear recursion of a sequence having linear complexity $l$ just from observing $2l$ consecutive bits of the sequence [1], the linear complexity of a sequence is a widely accepted measure of its unpredictability.

Linear complexity has been studied by various authors [2–4]. Two remarkable works in the study of the linear complexity of the resulting sequences are Key's paper [5] and Rueppel's root presence test for the product of distinct phases [6]. Although it does not appear explicitly in [5], the following result is generally known as Key's upper bound on the linear complexity.

"The linear complexity of the sequences obtained by any $k^{\text{th}}$-order filter function is upper bounded by $\sum_{l=1}^{k}\binom{L}{l}$."

On the other hand, Rueppel's root presence test for the product of distinct phases [6] allows the analysation of the contribution of every cyclotomic coset to the linear complexity of the sequences obtained by any $k^{\text{th}}$-order filter function $f$ with a single maximum order term $s_{n+t_0}s_{n+t_1}\cdots s_{n+t_{k-1}}$. This test can be stated as follows.

"Let $\alpha \in GF(2^L)$ be a root of the minimal polynomial of the sequence produced by the LFSR of length $L$. Then $\alpha^e = \alpha^{2^{e_0}+2^{e_1}+\cdots+2^{e_{k-1}}}$, $0 \le e_0 < e_1 < \cdots < e_{k-1} < L$ is a root of the minimal

The author thanks A. Fúster-Sabater for her valuable comments and suggestions about this work.


PII: S0898-1221(99)00331-4

polynomial of the sequence generated by $f$ if and only if the determinant

$$A_e = \begin{vmatrix} \alpha^{t_0 2^{e_0}} & \alpha^{t_1 2^{e_0}} & \cdots & \alpha^{t_{k-1} 2^{e_0}} \\ \alpha^{t_0 2^{e_1}} & \alpha^{t_1 2^{e_1}} & \cdots & \alpha^{t_{k-1} 2^{e_1}} \\ \cdot & \cdot & \cdots & \cdot \\ \alpha^{t_0 2^{e_{k-1}}} & \alpha^{t_1 2^{e_{k-1}}} & \cdots & \alpha^{t_{k-1} 2^{e_{k-1}}} \end{vmatrix} \neq 0."$$

If the determinant $A_e$ equals zero, then the corresponding cyclotomic coset is said to be degenerate for the function $f$. The determinant $A_e$ depends on three factors: the nonlinear filter function $f$, the minimal polynomial of the maximal-length LFSR, and the cyclotomic coset whose contribution is analysed.

This work provides new upper bounds on the linear complexity of binary sequences produced by certain families of nonlinear filter functions with a single maximum order term. The bases of the presented results are the root presence test and a new broad collection of cyclotomic cosets that are introduced and studied in Section 2. The degeneration of these new cosets is easily proved for certain families of nonlinear filter functions. That fact, in Section 3, is used to obtain new upper bounds for the linear complexity of the resulting sequences that improve upon Key's upper bound. The most remarkable contribution of the present work is that the proved results provide a practical and simple recommendation for the design of secure filter generators.

## 2. REGULAR COSETS

In this section, we introduce and analyse a new class of cyclotomic cosets, the so-called regular cosets, which constitute the starting point of the work. Some fundamental notation and a few definitions are introduced before the results can be stated and proved.

Since our concern is with binary sequences, most of the expressions discussed in this work will be over $GF(2)$, the finite field with two elements.

Let $(L,k)_c$ denote the $c^{\text{th}}$ common divisor of $L$ and $k$.

It is well known [7] that the integers in $\{1,2,\ldots,2^L-2\}$ that are relatively prime to $2^L-1$ form a group under multiplication modulo $2^L-1$, and the subset $\{1,2,2^2,\ldots,2^{L-1}\}$ forms a subgroup. This subgroup, when multiplied by any other element of the group, yields a so-called *proper coset.* In addition to these proper cosets, there are always one or more *improper cosets* that result from multiplying all the elements of the subgroup by an integer which is not relatively prime to $2^L-1$. The set of all cosets (proper and improper) of the multiplier subgroup constitutes the so-called *cyclotomic cosets* modulo $2^L-1$.

Let *coset* $e$ denote the cyclotomic coset $\{e, e2, e2^2, \ldots, e2^{L-1}\}$ (modulo $2^L-1$) that contains the integer $e$. Note that in the corresponding binary representation, coset $e$ consists of all the successive circular shifts of any of its $L$-bit strings. Throughout this work, the decimal form of the cosets' elements $2^{e_0}+2^{e_1}+\cdots+2^{e_{k-1}}$, $0 \le e_0 < e_1 < \cdots < e_{k-1} < L$, or their binary representation as $L$-bit strings of Hamming weight $k$ will be used indistinctly.

DEFINITION. *A cyclotomic coset modulo $2^L-1$ whose cardinality is less than $L$ is called a regular coset. In other words, a regular coset $e$ is a set of the form $\{e, e2, \ldots, e2^{m-1}\}$ (mod $2^L-1$), where the smallest positive integer $m$ such that $e2^m \equiv e \pmod{2^L-1}$ is smaller than $L$.*

The next result establishes a simple relation between regular and improper cosets.

LEMMA 1. *Every regular coset is an improper coset.*

PROOF. Let us proceed by contradiction by assuming that a regular coset $e$ is a proper coset. Thus, since $e$ would be relatively prime to $2^L-1$, then for all $m < L$, we have that $e(2^m-1) \not\equiv 0 \pmod{2^L-1}$, and the coset $e$ would not be a regular coset. ∎

The converse of Lemma 1 may not be true (see Example 1).

One of the most important points of any regular coset is that its elements can be represented as binary strings of length $L$ containing $k$ ones whose period is smaller than $L$. Regular cosets'

elements are called regular strings. This name is due to the regular distribution of the $k$ ones in the corresponding binary representations.

The next remark is useful for characterizing regular strings.

REMARK 1. Note that the period of the ones in any regular string strictly divides gcd $(L,k)$. Concretely, every regular $L$-bit string of Hamming weight $k$ is composed of $(L,k)_c$ repetitions of the same nonregular $L/((L,k)_c)$-bit string of Hamming weight $k/(L,k)_c$, and belongs to a regular coset whose cardinality is $L/(L,k)_c$. Thus, if $L$ and $k$ are relatively prime, there does not exist any regular coset. On the other hand, if $L$ and $k$ have some factor in common, then each common divisor of $L$ and $k$, $(L,k)_c$, determines a different collection $E^c$ of regular strings $e$ of the form

$$e = 2^{e_0} + 2^{e_1} + \cdots + 2^{e_{k-1}}, \qquad \text{such that } 0 \le e_0 < e_1 < \cdots < e_{k-1} < L,$$
$$\text{for all } i = 0,1,\ldots,\frac{k}{(L,k)_c} - 1, \quad \text{and for all } j = 1,2,\ldots,(L,k)_c - 1,$$
$$e_{i+j(k/(L,k)_c)} = e_i + j\frac{L}{(L,k)_c}.$$

In particular, one of those strings, $e^c$, is considered here the representative element of the collection $E^c$, and verifies the following expression:

$$e^c = 2^{e_0} + 2^{e_1} + \cdots + 2^{e_{k-1}}, \qquad \text{such that } 0 \le e_0 < e_1 < \cdots < e_{k-1} < L,$$
$$\text{for all } i = 0,1,\ldots,\frac{k}{(L,k)_c} - 1, \quad \text{and for all } j = 1,2,\ldots,(L,k)_c - 1,$$
$$e_i = i \qquad \text{and} \qquad e_{i+j(k/(L,k)_c)} = i + j\frac{L}{(L,k)_c}. \quad \blacksquare$$

From the precedent remark, a simple characterization of $e^c$ can be derived.

LEMMA 2. *Let $L$ and $k$ be integers. Then, the regular string $e^c$ can be expressed as the integer*

$$e^c = \left(2^{k/(L,k)_c} - 1\right)\frac{2^L - 1}{2^{L/(L,k)_c} - 1}.$$

PROOF. From the previous remark, it is easily deduced that the binary representation of $e^c$ is composed of $(L,k)_c$ repetitions of the same $L/(L,k)_c$-bit string with $k/(L,k)_c$ consecutive ones. The trick of the proof is that the contribution of the $j^{\text{th}}$ string $(j = 1,2,\ldots,(L,k)_c)$ to the integer $e^c$ is given by $(2^{k/(L,k)_c} - 1)$, $2^{(j-1)(L/(L,k)_c)}$, for all $j = 1,2,\ldots,(L,k)_c$. Since

$$1 + \frac{2^{L/(L,k)_c}\left(2^{L-L/(L,k)_c} - 1\right)}{2^{L/(L,k)_c} - 1}$$

is the sum of the $(L,k)_c$ first terms of a geometric progression with ratio $2^{L/(L,k)_c}$, then

$$e^c = \left(2^{k/(L,k)_c} - 1\right)\frac{2^L - 1}{2^{L/(L,k)_c} - 1}. \quad \blacksquare$$

From the particular structure of regular strings, it may be easily deduced that there exists a 1–1 correspondence between each regular $L$-bit string of Hamming weight $k$ determined by $(L,k)_c$ and each nonregular $L/(L,k)_c$-bit string of Hamming weight $k/(L,k)_c$. This idea leads us to next proposition that provides the total number of distinct regular strings related to a common divisor of $L$ and $k$.

PROPOSITION 1. *The number of distinct regular $L$-bit strings of Hamming weight $k$ belonging to the collection $E^c$ is given by the recursive expression*

$$|E^c| = \left( \begin{array}{c} \dfrac{L}{(L,k)_c} \\ \dfrac{k}{(L,k)_c} \end{array} \right) - \sum_{d \in D} |E^d|,$$

*where $D = \{d : (L,k)_d > (L,k)_c$ such that $(L,k)_c \mid (L,k)_d\}$, and if $(L,k)_c = \gcd(L,k)$, then*

$$|E^c| = \left( \begin{array}{c} \dfrac{L}{\gcd(L,k)} \\ \dfrac{k}{\gcd(L,k)} \end{array} \right).$$

In the expression of this last result, for every common divisor $(L,k)_c$, the total number of regular strings related to each common divisor that is a multiple of $(L,k)_c$ is subtracted to obtain the number of regular strings belonging to the collection $E^c$. The recursive formula of Proposition 1 may be easily expressed in a nonrecursive way by means of the prime factorization of the greatest common divisor of $L$ and $k$.

PROPOSITION 2. *Let $\gcd(L,k) = \prod_{r=1}^{m} p_r^{e_r}$ be the prime factorization of the greatest common divisor of $L$ and $k$. Then, the total number of distinct regular $L$-bit strings of Hamming weight $k$ is given by*

$$\sum_{J \subseteq \{1,2,\ldots,m\}} (-1)^{|J|+1} \left( \begin{array}{c} \dfrac{L}{\prod_{j \in J} p_j} \\ \dfrac{k}{\prod_{j \in J} p_j} \end{array} \right).$$

PROOF. The total number of distinct regular $L$-bit strings of Hamming weight $k$ is given by $\sum_c |E^c|$. Since $\gcd(L,k) = \prod_{r=1}^{m} p_r^{e_r}$, then every common divisor of $L$ and $k$ is a product of powers of prime numbers $p_r$. Then, by Proposition 1, we have that

$$\begin{aligned} \sum_c |E^c| &= \sum_{r=1}^{m} \left( \begin{array}{c} \dfrac{L}{p_r} \\ \dfrac{k}{p_r} \end{array} \right) + \left[ 1 - \binom{2}{1} \right] \sum_{\substack{\{d:(L,k)_d = \prod_{j \in J} p_j^{f_j}, \\ |J|=2, f_j \le e_j\}}} |E^d| \\ &\quad + \cdots + \left[ 1 - \binom{m}{1} \right] \sum_{\substack{\{d:(L,k)_d = \prod_{r=1}^{m} p_r^{f_r}, \\ f_r \le e_r\}}} |E^d| \\ &= \sum_{r=1}^{m} \left( \begin{array}{c} \dfrac{L}{p_r} \\ \dfrac{k}{p_r} \end{array} \right) + \left[ 1 - \binom{2}{1} \right] \sum_{\substack{J \subseteq \{1,2,\ldots,m\} \\ |J|=2}} \left( \begin{array}{c} \dfrac{L}{\prod_{j \in J} p_j} \\ \dfrac{k}{\prod_{j \in J} p_j} \end{array} \right) \\ &\quad + \cdots + \left[ 1 - \binom{m}{1} + \cdots + (-1)^{m-1} \binom{m}{m-1} \right] \left( \begin{array}{c} \dfrac{L}{\prod_{r=1}^{m} p_r} \\ \dfrac{k}{\prod_{r=1}^{m} p_r} \end{array} \right). \end{aligned}$$

Thus, since $1-\binom{r}{1}+\binom{r}{2}-\cdots+(-1)^{r-1}\binom{r}{r-1}=(-1)^{r-1}$, the number of regular strings is given by

$$\sum_{r=1}^{m}\binom{\frac{L}{p_r}}{\frac{k}{p_r}}-\sum_{\substack{J\subseteq\{1,2,\ldots,m\}\\|J|=2}}\binom{\frac{L}{\prod_{j\in J}p_j}}{\frac{k}{\prod_{j\in J}p_j}}+\cdots+(-1)^{m-1}\binom{\frac{L}{\prod_{r=1}^{m}p_r}}{\frac{k}{\prod_{r=1}^{m}p_r}}. \quad \blacksquare$$

Finally, certain values of $L$ and $k$ allow us to obtain an extremely simple expression of the total number of regular strings, that will be useful in the next section to establish a tight and suitable upper bound on the linear complexity of certain sequences.

COROLLARY 1. *If the greatest common divisor of $L$ and $k$ is the power of a prime number $p$, then the total number of distinct regular $L$-bit strings of Hamming weight $k$ is given by the binomial coefficient*

$$\binom{\frac{L}{p}}{\frac{k}{p}}.$$

The previous results are used in the next section to provide upper bounds on the linear complexity of sequences produced by certain nonlinear filter generators. This section ends with an example.

EXAMPLE 1. Consider the case $L=12$, $k=6$. First, note that not all the improper cosets are regular cosets. A counterexample of this could be the cyclotomic coset {63, 126, 252, 504, 1008, 2016, 4032, 3969, 3843, 3591, 3087, 2079}, that is improper because 63 is not relatively prime to $2^{12}-1$, but that is not regular because the coset's cardinality is 12.

The numbers 12 and 6 have three common divisors; they are $(12,6)_1=2$, $(12,6)_2=3$, and $(12,6)_3=6$, so there are three different collections of regular strings, represented, respectively, by the elements $e^1=2^0+2^1+2^2+2^6+2^7+2^8=455$, $e^2=2^0+2^1+2^4+2^5+2^8+2^9=819$, and $e^3=2^0+2^2+2^4+2^6+2^8+2^{10}=1365$. From Proposition 1, the number of distinct regular strings in each collection is given, respectively, by

$$|E^1|=\binom{6}{3}-2=18,$$

$$|E^2|=\binom{4}{2}-2=4,$$

and

$$|E^3|=\binom{2}{1}=2.$$

These collections are composed of the following regular cosets. There are three regular cosets in $E^1$; they are {455, 910, 1820, 3640, 3185, 2275}$\simeq${000111000111, 001110001110, ..., 100011100011}, {715, 1430, 2860, 1625, 3250, 2405} $\simeq$ {001011001011, 010110010110, ..., 100101100101}, and {1235, 2470, 845, 1690, 3380, 2665} $\simeq$ {010011010011, 100110100110, ..., 101001101001}.

Belonging, respectively, to $E^2$ and $E^3$ are the regular cosets {819, 1638, 3276,2457} $\simeq$ {001100110011, 011001100110, 110011001100, 100110011001} and {1365, 2730} $\simeq$ {010101010101, 101010101010}.

Thus, by Proposition 2, it is known that the total number of regular 12-bit strings of Hamming weight 6 is $\binom{6}{3}+\binom{4}{2}-\binom{2}{1}=24$. $\blacksquare$

## 3. UPPER BOUNDS

In this section, the root presence test is applied to regular cosets introduced in the last section, establishing some conditions under which the corresponding determinants are equal to zero. In this way, the last results on the numbers of regular cosets allow us to derive new upper bounds on the linear complexity of different families of nonlinear filter functions with a single maximum order term.

The next result provides a slight improvement of Key's upper bound for a large range of nonlinear functions.

THEOREM 1. *Let $f$ be a nonlinear filter function whose single maximum order term is the product $s_{n+t_0}s_{n+t_1}\cdots s_{n+t_{k-1}}$ and $\alpha \in GF(2^L)$ be a root of the minimal polynomial of the sequence produced by the LFSR of length $L$. If $k|L$ and there exist two different integers $i, j \in \{0,1,\ldots,k-1\}$ such that $\alpha^{t_i}, \alpha^{t_j} \in GF(2^{L/k})$, then the linear complexity of the sequences produced by $f$ satisfies the upper bound*

$$\left[\sum_{l=1}^{k}\binom{L}{l}\right] - \frac{L}{k}.$$

PROOF. According to the hypothesis, $\alpha^{t_i}, \alpha^{t_j} \in GF(2^{L/k})$, so we have that $\alpha^{t_i} \equiv \alpha^{t_i 2^{L/k}} \equiv \alpha^{t_i 2^{2L/k}} \equiv \cdots \equiv \alpha^{t_i 2^{(k-1)L/k}}$ in $GF(2^L)$ and $\alpha^{t_j} \equiv \alpha^{t_j 2^{L/k}} \equiv \alpha^{t_j 2^{2L/k}} \equiv \cdots \equiv \alpha^{t_j 2^{(k-1)L/k}}$ in $GF(2^L)$. Consequently, if the root presence test is applied to the regular coset $e$, where $e$ is of the form $e = 2^0 + 2^{L/k} + 2^{2L/k} + \cdots + 2^{(k-1)L/k}$, then the particular determinant $A_e$ equals zero since it has two columns linearly dependent over $GF(2^L)$. This fact implies that the regular coset $e$ does not contribute to the linear complexity of $f$ and the Key's upper bound may be diminished in its cardinality, that is $L/k$. ∎

EXAMPLE 2. Now consider $L = 8$, $k = 4$, the product $s_n\, s_{n+17}\, s_{n+18}\, s_{n+85}$, and $\alpha \in GF(2^8)$ a root of the minimal polynomial of a sequence produced by the LFSR of length 8. Since $4|8$ and $\alpha^0, \alpha^{85} \in GF(2^2)$, then the regular coset corresponding to the common divisor 4, {85, 170} is degenerate for $f$. ∎

Now, by using Proposition 2, the upper bound of Theorem 1 can be improved for a family of filter functions that satisfy stronger restrictions.

THEOREM 2. (MAIN THEOREM). *Let $f$ be a nonlinear filter function whose single maximum order term is the product $s_{n+t_0}s_{n+t_1}\cdots s_{n+t_{k-1}}$, $\alpha \in GF(2^L)$ be a root of the minimal polynomial of the sequence produced by the LFSR of length $L$, and $\gcd(L,k) = \prod_{r=1}^{m} p_r^{e_r}$ be the prime factorization of the greatest common divisor of $L$ and $k$. If for every $r \in \{1,2,\ldots,m\}$, there exist $k/p_r + 1$ different values of $i \in \{0,1,\ldots,k-1\}$ such that $\alpha^{t_i} \in GF(2^{L/p_r})$, then the linear complexity of the sequences produced by $f$ satisfies the upper bound*

$$\sum_{l=1}^{k}\binom{L}{l} - \sum_{J\subseteq\{1,2,\ldots,m\}} (-1)^{|J|+1} \binom{\dfrac{L}{\prod_{j\in J} p_j}}{\dfrac{k}{\prod_{j\in J} p_j}}.$$

PROOF. Consider all the corresponding regular cosets related to each common divisor of $L$ and $k$. By Remark 1, we know that for every regular coset $e$ corresponding to a prime number $p_r$ or one of its multiples, for all $i = 0,1,\ldots,k/p_r-1$, and for all $j = 1,2,\ldots,p_r-1$, $e_{i+j(k/p_r)} = e_i + j(L/p_r)$. On the other hand, by hypothesis, we have that for every $r \in \{1,2,\ldots,m\}$, there exist $k/p_r + 1$ different values of $i \in \{0,1,\ldots,k-1\}$ such that $\alpha^{t_i} \in GF(2^{L/p_r})$, so the determinant $A_e$ can be

computed by expanding it along $k - k/p_r - 1$ columns. In this way, $A_e$ may be written as a linear combination of adjuncts of order $k/p_r + 1$, every one with two identical rows. Consequently, every $A_e$ equals zero and no regular coset contributes to the linear complexity of the sequences produced by $f$. ∎

When the relation between $L$ and $k$ is of a particular form, the hypothesis of the previous theorem can be easily relaxed to involve a broader family of nonlinear functions. This is stated in the following result that makes use of Corollary 1.

COROLLARY 2. *Let $f$ be a nonlinear filter function whose single maximum order term is the product $s_{n+t_0}s_{n+t_1}\cdots s_{n+t_{k-1}}$, $\alpha \in GF(2^L)$ be a root of the minimal polynomial of the sequence produced by the LFSR of length $L$, and $L$ and $k$ such that their greatest common divisor is the power of a prime number $p$. If for every $i = 0, 1, \ldots, k/p$, the power $\alpha^{t_i} \in GF(2^{L/p})$ , then the linear complexity of the sequences produced by $f$ satisfies the upper bound*

$$\sum_{l=1}^{k}\binom{L}{l} - \binom{\frac{L}{p}}{\frac{k}{p}}.$$

By using simple tools of combinatorial calculus, it is easy to prove that the number of functions under the conditions of Theorem 2 is very large.

PROPOSITION 3. *The number of products under the conditions of Theorem 2 is*

$$\binom{2^L - 2 - \sum_{r=1}^{m}\frac{k}{p_r}}{k - 1 - \sum_{r=1}^{m}\frac{k}{p_r}} \prod_{r=1}^{m}\binom{2^{L/p_r} - 2}{\frac{k}{p_r}}.$$

EXAMPLE 3. Let $L = 8$, $k = 4, \alpha$ be a primitive element of $GF(2^8)$, $GF(2^4)$= $\{0, 1, \alpha^{17}, \alpha^{34}, \alpha^{68}, \alpha^{136}, \alpha^{85}, \alpha^{170}, \alpha^{102}, \alpha^{204}, \alpha^{153}, \alpha^{51}, \alpha^{187}, \alpha^{119}, \alpha^{238}, \alpha^{221}\}$ and $f$ be any nonlinear filter function whose single maximum order term is one of the $\binom{15}{3}\binom{252}{1} = 114.660$ products of the set $\{\{s_n s_{n+17}\ s_{n+34}\ s_{n+t_3}/\ t_3 \notin \{0, 17, 34\}, \ldots, \{s_{n+119}s_{n+238}\ s_{n+221}\ s_{n+t_3}/\ t_3 \notin \{119, 238, 221\}\}$. Then, by Corollary 2, the linear complexity of the sequences produced by $f$ is guaranteed to be at most

$$\binom{8}{1} + \binom{8}{2} + \binom{8}{3} + \binom{8}{4} - \binom{4}{2} = 156.$$ ∎

REMARK 2. From the above results, we may conclude that using nonlinear filter generators whose values of $L$ (length of the LFSR) and $k$ (order of the filter function) are not relatively prime could be indeed dangerous, because in that case, regular cosets described in this work could produce a great decrease in the linear complexity of the resulting sequences. This decrease implies not only the nonoptimality of generators under the hypothesis of the theorems, but also of other generators with the same LFSRs and similar nonlinear filter functions because the difference between sequences produced by both types of generators may be in only one position of a period, whereas the difference in their linear complexities may be high. Thus, many filter generators with values of $L$ and $k$ not relatively prime could have bad linear-complexity stability [8]. Table 1 shows some values of $L$ and $k$, and the approximate decrease of Key's upper bound derived from the degeneration of all the regular cosets. Note that for practical values such as $L = 128$ and $k = 64$, this approximate decrease is large, $10^{18}$. Furthermore, decreases described here could be added to any other decrease produced by the degeneration of other kinds of cyclotomic cosets. ∎

Table 1. Decrease of Key's upper bound.

| $L$ | 24 | 60 | 84 | 126 | 128 | 140 | 210 | 420 |
|---|---|---|---|---|---|---|---|---|
| $k$ | 12 | 30 | 42 | 42 | 64 | 70 | 70 | 210 |
| Decrease | 988 | $10^8$ | $10^{11}$ | $10^{16}$ | $10^{18}$ | $10^{20}$ | $10^{27}$ | $10^{61}$ |

## 4. CONCLUSIONS

This paper gives some specific conditions under which Key's upper bound on the linear complexity of nonlinear filter generators cannot be reached. The main result is based on the proved degeneration of a new broad collection of cyclotomic cosets introduced in this work. A slight improvement of Key's upper bound is presented and its effectiveness is suggested by a simple recommendation for the choice of the length of the LFSR and the order of the filter function that is proposed as a design principle for filter generators. The problem of finding other kinds of cyclotomic cosets whose degeneration could be proved for the same families of nonlinear filter functions described here is a part of a work in progress.

## REFERENCES

1. J.L. Massey, Shift register synthesis and BCH decoding, *IEEE Transactions on Information Theory* **IT-15**, 122–127 (1969).
2. Z.D. Dai, T. Beth and D. Gollmann, Lower bounds for the linear complexity of sequences over residue rings, In *Advances in Cryptology-Eurocrypt '90*, Lecture Notes in Computer Science, Volume 473, Springer-Verlag, (1991).
3. A. Fúster-Sabater and P. Caballero-Gil, On the linear complexity of nonlinearly filtered PN-sequences, In *Advances in Cryptology-Asiacrypt '94*, Lecture Notes in Computer Science, Volume 917, Springer-Verlag, (1995).
4. H. Niederreiter, The linear complexity profile and the jump complexity of keystream sequences, In *Advances in Cryptology-Asiacrypt '90*, Lecture Notes in Computer Science, Volume 473, Springer-Verlag, (1991).
5. E.L. Key, An analysis of the structure and complexity of nonlinear binary sequence generators, *IEEE Transactions on Information Theory* **IT-22**, 732–736 (1976).
6. R.A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, (1986).
7. S.W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, CA, (1967); Revised edition, Aegean Park Press, Laguna Hills, CA, (1982).
8. C. Ding, G. Xiao and W. Shan, *The Stability Theory of Stream Ciphers*, Lecture Notes in Computer Science, Volume 561, Springer-Verlag, (1991).