



SDI Review Form 1.6

Journal Name:	British Journal of Mathematics & Computer Science
Manuscript Number:	Ms_BJMCS_19442
Title of the Manuscript:	Construction of Maximum period Linear Feedback Shift Registers (LFSR) (Primitive polynomials and linear recurring relations)
Type of the Article	Original Research Article

General guideline for Peer Review process:

This journal's peer review policy states that **NO** manuscript should be rejected only on the basis of '**lack of Novelty**', provided the manuscript is scientifically robust and technically sound.

To know the complete guideline for Peer Review process, reviewers are requested to visit this link:

(<http://www.sciencedomain.org/page.php?id=sdi-general-editorial-policy#Peer-Review-Guideline>)



SDI Review Form 1.6

PART 1: Review Comments

	Reviewer's comment	Author's comment (if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)
<u>Compulsory</u> REVISION comments	The author is kindly asked to explain the original contribution of his work. Otherwise, in the actual form, this manuscript seems to be a review paper, not an original research paper.	The problem is addressed in the summary of the paper (P.1- Abstract)), and at paragraph 5: conclusion. As indicated, the proposed method determines mathematically, from the primitive polynomial, linear recurring relation generating the LFSR (and vice versa), and thus facilitate its construction; it also help to establish the corresponding reciprocal primitive polynomial which gives the possibility to build another LFSR as good as the first. We have a design and a careful choice of maximum length LFSR to use, on the basis of the primitive polynomial, the reciprocal polynomial and associated linear recurring relations, that do not show the methods used so far where the linear recurring relations are established, without further details, from the primitive polynomials to draw the LFSR. On the other hand, it seemed important to review the FSR and to emphasize their cryptographic security with recommendations and perspectives of research in this area.
<u>Minor</u> REVISION comments	P.1, in the Introduction: "Contrary to the blocks ciphers..."(please delete "In"). P.2: lines 1 and 2, please delete the second open parenthesis. P.2: "The two (2) methods are...in [19], [29],..."(please add "in"). P.3: missing point in the end of a phrase. P.3: please revise the notations: $F = \{0,1\}^n$ with values in $\{0,1\}$. This contradicts the definition of F, which is $\{0,1\}^{(n+1)}$ -	All corrections have been done P.3: the notations is : $F = \{0,1\}^n$ with values in $\{0,1\}^n$ (This is a typing error); In formula 1, the variable too is deleted (x 1), and clarifications have been made in the formulas at the end of page (P.3)



SDI Review Form 1.6

	valued. The usual notation is $F: \{0,1\}^n \rightarrow \{0,1\}^{(n+1)}$. P.5: "Alternatively, we can use...recurrences to generate..." (Please delete "is used", in order to avoid repeating words). P. 12, line 3: $F(x)=x^n+(a_0)*x^{(n-1)}+...+(a_i)*x^{(n-i-1)}+...+a_{(n-1)}$ (Please do the correction marked in red). There are some phrases which have no sense. Please revise the English wording.	The polynomial $f(x)$ is finally represented in his normal form as indicated at page 10 of the paper (2.4 Theorem) corrections have been done
<u>Optional/General</u> comments	The first Referee of this work should be a specialist in this field (algebra, primitive polynomials, encoding-decoding procedures).	The necessary steps have been taken in this regard