Comments on "A Family of Keystream Generators with Large Linear Complexity"

A. FÚSTER-SABATER
Instituto de Física Aplicada, C.S.I.C.
Serrano 144, 28006 Madrid, Spain
amparo@iec.csic.es

(Received July 2001; accepted October 2002)

Abstract—In these comments, it is shown that the family of keystream generators, lower bound on the linear complexity and computation procedure followed by the authors in [1] coincide with the family of keystream generators, lower bound on the linear complexity nd computation procedure previously followed by Rueppel in [2]. © 2004 Elsevier Ltd. All rights reserved.

Keywords—Nonlinear filter, LFSR-based generator, Linear complexity, Stream cipher.

In the above work [1], a family of $m$th-order nonlinear filters applied to the stages of a LFSR of length $L$ is considered. The generic nonlinear filter function of this family has a unique term product of $m$ equidistant phases of the same PN-sequence of the form

$$f = a_{n+t_1} \cdot a_{n+t_2} \cdots a_{n+t_m}$$

with $t_i = 2^k \cdot i \cdot \vartheta$ where $k, i, \vartheta \in N$ and $\gcd(\vartheta, 2^L - 1) = 1$. The linear complexity of the resulting sequence is analyzed and a lower bound on the linear complexity value is provided. In order to derive such a lower bound, the authors make use of the root presence test for the product of distinct phases of a PN-sequence, $A_e \neq 0$ [2, Chapter 5, p. 78, Proposition 5.5].

In reference [2, Chapter 5, p. 83, Corollary 5.6], cited by the authors in [1], Rueppel defines a family of keystream generators whose generic nonlinear function is $f$ in equation (1) with

$$t_i = i \cdot \vartheta \quad \text{and} \quad \gcd (\vartheta, 2^L - 1) = 1.$$  \hspace{1cm} (2)

By means of the root presence test and expressing $A_e$ as a Vandermonde determinant, the author gives a lower bound on the linear complexity of the generated sequence of value $\binom{L}{m}$.

In the above work [1], the authors define a family of keystream generators whose generic nonlinear filter function is $f$ in equation (1) with

$$t_i = 2^k \cdot i \cdot \vartheta \quad \text{and} \quad \gcd (\vartheta, 2^L - 1) = 1.$$  \hspace{1cm} (3)

Comments supported by Ministerio de Ciencia y Tecnología (Spain) under Grant TIC 2001-0586.
By means of the root presence test and expressing $A_e$ as a Vandermonde determinant, the authors give a lower bound on the linear complexity of the generated sequence of value $\binom{L}{m}$.

It is clear that if $t_i = 2^k \cdot i \cdot \theta = i \cdot \theta'$, then the condition $\gcd(\theta', 2^L - 1) = 1$ holds too, since if $\gcd(\theta, 2^L - 1) = 1$, then $\theta' = \theta \cdot 2^k$ will never divide $2^L - 1$. Thus, the nonlinear filters defined in [1] with

$$t_i = i \cdot \theta' \quad \text{and} \quad \gcd(\theta', 2^L - 1) = 1$$

are just the elements of the family of nonlinear filters with equidistant phases described by Rueppel in [2]. Multiplying by $2^k$ the distance between two consecutive phases does not define a new family of filter functions as the authors claim. In fact, they are just considering the nonlinear filters of the family of keystream generators characterized by Rueppel.

In brief, the authors of [1] have followed the same procedure followed by Rueppel in [2] to obtain the same lower bound obtained by Rueppel in [2] for the elements of the same family of filter functions defined by Rueppel in [2].

Lower bounds on the linear complexity for more general filter functions including lower-order terms or/and a linear combination of $m$-order terms with equidistant phases can also be found in [2, Chapter 5, pp. 84–86; 3].

Finally, the footnote in [1] is not correct either. In fact, the work presented at the rump session of Eurocrypt '99 [4] (with different authors and contents) introduced the concept of $2^k$-distant functions and their cryptographic properties. Neither the nonlinear filters with equidistant phases were considered there nor lower bounds on the linear complexity of nonlinear filters with equidistant phases were provided there.

REFERENCES