PRODUCTS OF LINEAR RECURRING SEQUENCE WITH MAXIMUM COMPLEXITY

Rainer A. Rueppel
University of California
San Diego, USA

Othmar J. Staffelbach
GRETAG AKTIENGESELLSCHAFT
Regensdorf, Switzerland

Abstract

A common type of running-key generator employed in stream cipher systems consists of n (mostly maximum-length) linear feedback shift registers (LFSRs) whose output sequences are combined in a nonlinear function F to produce the key stream.

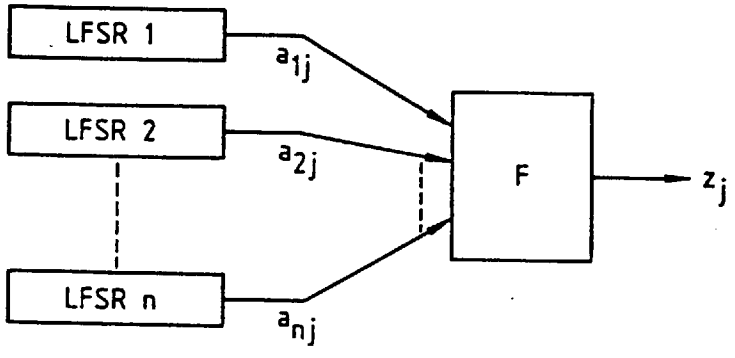

Figure 1: Common type of running-key generator

One of the major objectives of F is to increase the linear complexity of the key stream such that the synthesis of a linear equivalent of the running-key generator (e.g. by using the Berlekamp-Massey LFSR synthesis algorithm becomes computationally infeasible. Thus considerable interest has been paid to the problem of controlling the linear complexity of sequences that result from nonlinear combinations, in particular products, of LFSR-sequences.

The linear complexity of a product sequence can never exceed the product of the linear complexities of the sequences being multiplied. Consequently, if the linear complexity of a product sequence satisfies this upper bound with equality, we shall say that this product sequence attains **maximum linear complexity**. At least since the work of Selmer, it has been known that

The product of two GF(q)-sequences with irreducible minimal polynomials of degrees L and M, respectively, attains maximum linear complexity LM if L and M are relatively prime. Consequently, most running-key generators of the type depicted in Figure 1 are built according to this condition; the driving LFSRs usually have not only irreducible but also primitive connection polynomials, and their lengths are chosen to be pairwise relatively prime. We will show in this paper that neither irreducibility of the involved minimal polynomials nor relative primeness of their degrees is required to obtain maximum linear complexity.

We first consider the case where the sequences to be nonlinearly combined have irreducible minimal polynomials, but of arbitrary degrees. One of our main results under this assumption is that **the product of any number of maximum-length GF(q)-sequences attains maximum linear complexity provided only that the degrees of the minimal polynomials are different and greater than 2.** Our arguments rely on the fact that every number q^m-1, $m = 3,4,\ldots$, (with the sole exception $q = 2$, $m = 6$) has a primitive prime factor. A primitive factor of q^m-1 is defined as a divisor of q^m-1 which is relatively prime to every q^i-1, $1 \leq i < m$.

From the cryptographic viewpoint, a single product of many sequences is of little interest, since the resulting statistics tends to be poor. Consider therefore the case when n sequences with irreducible minimal polynomial are combined in a nonlinear function F of the form

$$F_n(x_1,\ldots,x_n) = a_0 + \sum a_i x_i + \sum a_{ij} x_i x_j + \ldots + a_{12..n} x_1 x_2 \ldots x_n \qquad (1)$$

$$a_0, a_i, a_{ij}, \ldots \in GF(q).$$

For $q = 2$, this is the general form of a Boolean function (the so-called algebraic normal form), but (1) describes a restricted class of functions when $q > 2$.

It is proved that any number of maximum-length GF(q)-LFSRs may be combined by a nonlinear function F as defined in (1) and provided only that the LFSRs have different lengths greater than 2, the resulting linear complexity may be directly computed by replacing the nonzero coefficients of F by 1 and

the sequence arguments of F by the corresponding LFSR-lengths, and by evaluating the resulting formula over the reals (instead of GF(q)). This rule of evaluating linear complexities was known to provide an upper bound on linear complexity in the general case.

When the assumption of irreducibility of the minimal polynomials is dropped, it will be shown that a product of two sequences attains maximum linear complexity if the roots of at least one minimal polynomial are pairwise linearly independent over the largest common subfield contained in the splitting fields of the minimal polynomials. This result can be generalized to nonlinear combinations (as defined in (1)) of n sequences whose minimal polynomials have only simple roots; especially under the assumption that the splitting fields of the minimal polynomials have pairwise relatively prime degrees over the groundfield GF(q), the resulting output sequence will have the maximum linear complexity allowed by F, provided only that all the roots are pairwise linearly independent over GF(q) (which is automatically satisfied when q = 2). Here neither irreducibility of the involved minimal polynomials nor pairwise relative primeness of their degrees is required to guarantee maximum linear complexity. But "the circle has been closed" in the sense that the degrees of the involved splitting fields have to be pairwise relatively prime. Note that the last condition allows in the binary case the achievement of extraordinarily high linear complexities since all but one element in an extension field may be used as roots of a minimal polynomial and therefore count in a product of maximum linear complexity.

Reference:

R.A. Rueppel, O.J. Staffelbach, "Products of Linear Recurring Sequences with Maximum Complexity", to appear in IEEE Trans. on Info. Theory.