Journal of Complexity 29 (2013) 173–181

Contents lists available at SciVerse ScienceDirect

Journal of Complexity

journal homepage: www.elsevier.com/locate/jco

On the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR☆

Zhen Ma, Wen-Feng Qi *, Tian Tian

Department of Applied Mathematics, Zhengzhou Information Science and Technology Institute, Zhengzhou, PR China

ARTICLE INFO

Article history:
Received 16 April 2012
Accepted 24 September 2012
Available online 2 October 2012

Keywords:
Stream ciphers
Nonlinear feedback shift registers
Cascade connection
Boolean functions
Linear complexity

ABSTRACT

In this paper, we study the decomposition of an NFSR into a cascade connection of an NFSR into an LFSR which is a kind of concatenation of an NFSR and an LFSR. It is shown that this problem can be solved based on polynomial factorization in $\mathbf{F}_2[x]$, and a potential weakness of an NFSR that can be decomposed in such a way is further discussed.

1. Introduction

With the development of correlation attacks and algebraic attacks, stream ciphers based on linear feedback shift registers (LFSRs) are facing more and more security problems. To resist these attacks, many recently proposed stream ciphers are designed based on nonlinear feedback shift registers (NFSRs). For example, many eSTREAM finalists use NFSRs as a building block, such as Grain [4], Mickey [1] and Trivium [2].

In general, an NFSR can be implemented either in the Fibonacci configuration (called Fibonacci NFSR for simplicity) or in the Galois configuration (called Galois NFSR for simplicity), and the Fibonacci configuration can be seen as a special case of the Galois configuration. In this paper, we are only concerned with Fibonacci NFSRs and Galois NFSRs which are the cascade connections of two Fibonacci NFSRs.

Let $h(x_0, \ldots, x_r) = h_0(x_0, \ldots, x_{r-1}) \oplus x_r$ be a Boolean function of $r+1$ variables. A diagram of an r-stage Fibonacci NFSR with characteristic function h is given in Fig. 1, denoted by NFSR(h). An output

☆ This work was supported by NSF of China under Grant No. (61272042, 61100202).
* Corresponding author.
E-mail addresses: zhen_ma@163.com (Z. Ma), wenfeng.qi@263.net (W.-F. Qi), tiantian_d@126.com (T. Tian).

0885-064X/$ – see front matter © 2013 Published by Elsevier Inc.
doi:10.1016/j.jco.2012.09.003

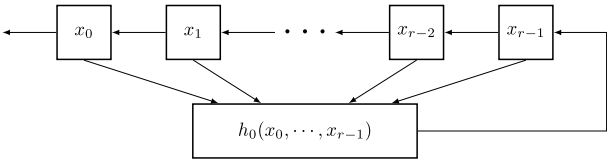

Fig. 1. An r-stage Fibonacci NFSR.

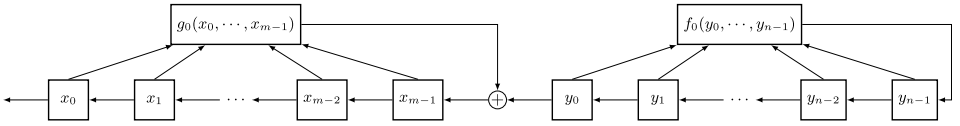

Fig. 2. The cascade connection of NFSR(f) into NFSR(g).

sequence $\underline{a}$ of the NFSR(h) satisfies the following recurrence relation

$$a_{k+r} = h_0(a_k, a_{k+1}, \ldots, a_{k+r-1}), \quad k \geq 0.$$

The set of all output sequences of the NFSR(h) is denoted by $G(h)$. In particular, if h is linear, then the NFSR(h) is actually an LFSR, and so it is also denoted by LFSR(h).

The notion of the cascade connection of two Fibonacci NFSRs was first proposed by Green and Dimond in [3], which was also called the product-feedback shift register. Let $f(x_0, \ldots, x_n) = f_0(x_0, \ldots, x_{n-1}) \oplus x_n$ be an n-variable Boolean function and let $g(x_0, \ldots, x_m) = g_0(x_0, \ldots, x_{m-1}) \oplus x_m$ be an m-variable Boolean function. The Galois NFSR shown in Fig. 2 is called the cascade connection of NFSR(f) into NFSR(g), which is denoted by NFSR(f, g). The output sequences of the register labeled x_0 is called the output sequences of NFSR(f, g) and the set of all output sequences of the NFSR(f, g) is denoted by $G(f, g)$.

The multiplication denoted by a dot "$\cdot$" in [3] and an asterisk "$*$" in [6]–[7] was introduced to investigate the characteristic function of the cascade connection of two NFSRs. We shall use the symbol "$*$" throughout the paper. For any two Boolean functions $f(x_0, \ldots, x_n)$ and $g(x_0, \ldots, x_m)$, define

$$f * g = f(g(x_0, \ldots, x_m), g(x_1, \ldots, x_{m+1}), \ldots, g(x_n, \ldots, x_{n+m})).$$

If f and g are characteristic functions of two Fibonacci NFSRs, respectively, then it is easy to see that $f * g$ is of the form

$$f * g = h_0(x_0, \ldots, x_{n+m-1}) \oplus x_{n+m},$$

a characteristic function of an NFSR, and it was shown in [3]–[6] that the NFSR(f, g) is equivalent to the NFSR($f * g$), i.e., $G(f, g) = G(f * g)$.

In this paper, we mainly study the decomposition of a Fibonacci NFSR into the cascade connection of a Fibonacci NFSR into an LFSR. Specifically, given a Boolean function h, we present a method to find all the linear Boolean functions l such that $h = f * l$ for some Boolean function f, where l is called a linear $*$-factor of h. Our result shows that all linear $*$-factors of h can be obtained by factoring a polynomial defined by h over the finite field $\mathbf{F}_2$. Furthermore, a potential weakness of an NFSR(h) equivalent to a cascade connection of an NFSR(f) into an LFSR(l) for cryptographic applications is discussed, i.e., $h = f * l$. It is proved that if a sequence in $G(f)$ has small linear complexity, then a subset of sequences in $G(f, l) = G(h)$ will have small linear complexities, whose number is equal to the number of sequences in $G(l)$. In particular, if $f(0, \ldots, 0) = 0$, then $G(l) \subseteq G(f * l)$. Therefore, for the sake of security, it is not advisable to design stream ciphers based on such NFSR(h). All our results are also true for an affine Boolean function l.

The rest of the paper is organized as follows. In Section 2 we present some necessary preliminaries. Section 3 gives the main results of the paper. In detail, in Section 3.1, for a Boolean function h, we give a linear Boolean function l_h defined by h such that the set of linear $*$-factors of h is contained in that