Finite Fields and Their Applications 38 (2016) 57–71

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A discrete logarithm-based approach to compute low-weight multiples of binary polynomials

Pietro Peterlongo, Massimiliano Sala *, Claudia Tinnirello *

Dipartimento di Matematica, Università di Trento, Via Sommarive 14, 38123 Trento, Italy

ARTICLE INFO

Article history:
Received 30 April 2015
Received in revised form 15 December 2015
Accepted 17 December 2015
Available online 6 January 2016
Communicated by D. Panario

MSC:
12Y05
11T71
11T55
12E05
68Q25

Keywords:
Parity check
Correlation attack
Stream cipher
Discrete logarithm

ABSTRACT

Being able to compute efficiently a low-weight multiple of a given binary polynomial is often a key ingredient of correlation attacks to LFSR-based stream ciphers. The best known general purpose algorithm is based on the generalized birthday problem. We describe an alternative approach which is based on discrete logarithms and can take advantage of the structure of the polynomial. In some cases it has much lower memory complexity requirements with a comparable time complexity.

* Corresponding authors.
E-mail addresses: maxsalacodes@gmail.com (M. Sala), claudia.tinnirello@gmail.com (C. Tinnirello).

http://dx.doi.org/10.1016/j.ffa.2015.12.005
1071-5797/

1. Introduction

A Linear Feedback Shift Register (LFSR) is the basic component of many keystream generators for stream ciphers applications. It is defined by its connection polynomial, which is a binary polynomial. A parity check for a single LFSR is a multiple of its connection polynomial, while a parity check for more than one LFSR is a multiple of the least common multiple of the respective connection polynomials. The weight of a parity check is the weight of the associated polynomial, that is, the number of its nonzero coefficients.

Correlation attacks were introduced by Siegenthaler in [1] to cryptanalyze a large class of stream ciphers based on LFSRs. A major improvement by Meier and Staffelbach [2] led to different versions of fast correlation attacks [3–5].

These attacks try to find a correlation between the output of the stream cipher and one of the LFSRs on which it is built, then they try to recover the state of the LFSR by decoding the keystream as a noisy version of the LFSR output. A fast version of a correlation attack involves the precomputation of multiple parity checks of one of the LFSRs in order to speed up the computation. This precomputation step can be performed according to two different approaches, one based on the birthday paradox [6] and another based on discrete logarithms [7]. The determination of an efficient algorithm for the computation of a polynomial multiple (subject to given constraints, e.g. on the degree) is an interesting problem in itself for computational algebra.

It might be argued that the design of modern stream ciphers evolved accordingly. A cipher like E0 [8] is not immediately subject to these types of attacks, since no apparently single LFSR is correlated to the keystream output. In [9], Lu and Vaudenay introduced a new fast correlation attack which is able to successfully recover the state of E0. Their attack requires a different precomputation step which computes a *single* parity check of *multiple* LFSRs. The complexity of their precomputation step is not far from the complexity of their full attack, and they employed the generalized birthday approach presented in [10]. Further research was recently presented in [11], which contains in particular a straightforward generalization of the discrete logarithm approach of [7].

In this paper we generalize the discrete log approach of [7], proposing an algorithm that is able to compute a single parity check of multiple LFSRs, obtaining thus the same goal as in [9] but without employing any birthday paradox method. To be more precise, the problem we will address throughout the paper is the following:

Problem 1 Find a given-weight polynomial multiple with target degree
Input: A polynomial p and two integers $w \geq 3$ and D.
Output: A multiple of p of weight w and degree at most D, if it exists.

In Section 2, we present our strategy, we fix the notation and we give algebraic results on which the algorithm is based. The algorithm we propose is explained in Section 3, along with a comparison of its complexity to the generalized birthday approach and to the straightforward generalization of the discrete log approach for the case of a single primitive polynomial. Significant examples of our approach are outlined in Subsection 3.3.1,