Finite Fields and Their Applications 47 (2017) 222–241

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Discrete linear models for the generalized self-shrunken sequences

Sara D. Cardell [a,*], Amparo Fúster-Sabater [b]

[a] *Instituto de Matemática, Estatística e Computação Científica, University of Campinas, R. Sérgio Buarque de Holanda, 651, 13083-859, Campinas, Brazil*
[b] *Instituto de Tecnologías Físicas y de la Información, Consejo Superior de Investigaciones Científicas, C/ Serrano, 144, 28006, Madrid, Spain*

ARTICLE INFO

Article history:
Received 2 February 2017
Received in revised form 1 June 2017
Accepted 2 June 2017
Available online xxxx
Communicated by Arne Winterhof

MSC:
68Q80
94A55

Keywords:
Modified self-shrinking generator
Generalized self-shrinking generator
Characteristic polynomial
Cellular automata
Decimation

ABSTRACT

In this work, different decimation-based sequence generators for cryptographic purposes have been analyzed in detail. In fact, the modified self-shrinking generator was first introduced as an improved version of the self-shrinking generator. However, it is here proven that the sequences produced by both generators belong to the same family of sequences, that is the class of the generalized self-shrinking sequences. Thus, both sequences have the same properties as well as the same weaknesses. Moreover, such sequences can be generated by linear structures based on one-dimensional cellular automata. The linearity inherent to the cellular automata-based models can be used to launch a cryptanalytic attack against such non-linear generators.

© 2017 Elsevier Inc. All rights reserved.

* Corresponding author.
E-mail addresses: sdcardell@ime.unicamp.br (S. D. Cardell), amparo@iec.csic.es (A. Fúster-Sabater).

http://dx.doi.org/10.1016/j.ffa.2017.06.010
1071-5797/© 2017 Elsevier Inc. All rights reserved.

1. Introduction

Private-key cryptographic systems are commonly classified into stream and block ciphers. Indeed, stream ciphers encrypt each plaintext bit into a ciphertext bit under a time varying transformation (varying key) while block ciphers encrypt an entire block of plaintext bits at a time with the same key (static key) [1].

The basic problem in stream ciphers design is to generate from a short and truly random key a long pseudo-random sequence of bits called the keystream sequence. For encryption, the sender performs the bitwise XOR operation among the bits of the original message or plaintext and the keystream sequence. The result is the ciphertext to be sent to the receiver. For decryption, the receiver generates the same keystream, performs the same bitwise XOR operation between the received ciphertext and the keystream sequence and recovers the original message.

Most keystream generators are based on maximal-length Linear Feedback Shift Registers (LFSRs) [2] whose output sequences, the so-called m-sequences, are combined by means of nonlinear functions in order to: a) break the inherent linearity of such sequences and b) produce keystream sequences for cryptographic applications.

One of the most popular and well known families of keystream generators is the class of decimation-based sequence generators. The basic idea of this kind of generators is the irregular decimation of an m-sequence according to the bits of another one. The result of this decimation is a new sequence that will be used as keystream sequence in stream ciphers. Inside this family of generators, we can describe the following examples.

The shrinking generator, first introduced in [3], is a keystream generator based on the irregular decimation of two m-sequences. One year later, Meier and Staffelbach introduced the self-shrinking generator [4], a simpler structure using one LFSR whose output sequence is shrunken in the same way as that of the shrinking generator. Years later, the modified self-shrinking generator was introduced by Kanso in [5] as an improved version of the self-shrinking generator. In the meanwhile, the generalized self-shrinking generator introduced in [6] is defined as a simple keystream generator that produces a family of decimated sequences, which includes the output sequence obtained from the self-shrinking generator.

On the other hand, binary sequences generated by a kind of one-dimensional linear cellular automaton (CA) have been found to be exactly the same m-sequences as those of the maximal-length LFSRs. In this sense cellular automata can be considered as alternative generators of m-sequences. The relevance of these automata is due to the fact that some cryptographic generators designed as LFSR-based nonlinear structures can be modelled as CA-based linear structures. In fact, the shrinking and self-shrinking generators have been already modelled using linear 102-CA and 150-90-CA [7–10]. Furthermore, the generalized self-shrinking generator was modelled using 150-90-CAs in [11]. In this work, a new family of 102-CAs that model the generalized self-shrunken sequences is introduced, i.e., every sequence produced by this generator can be obtained as an output sequence of linear 102-CA. Besides, we show that the modified self-shrinking generator

Download English Version:

https://daneshyari.com/en/article/5771620

Download Persian Version:

https://daneshyari.com/article/5771620

Daneshyari.com