Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 123 (2018) 203–211

Procedia Computer Science

www.elsevier.com/locate/procedia

8th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2017

Non-Binary Pseudorandom Number Generators For Information Security Purposes

Ivanov M.A., Roslyj E.B., Starikovskiy A.V., Krasnikova S.A., Shevchenko N.A., Shustova L.I.

National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute)
Kashirskoe highway 31, 115409, Moscow, Russian Federation
maivanov@mephi.ru

Abstract

The paper considers non-binary pseudorandom number generators (PRNG) on the non-linear feedback shift registers (NLFSR). The schemes of p-ary NLFSR are given that create a sequence of length $S \leq p^N$, where N is a degree of a primitive polynomial over GF(p)). In addition, the scheme of the universal NLFSR is given, which generates, depending on configuration, the sequences of any period including the maximum possible for a given amount of memory elements. The peculiarity of the considered NLFSR is the presence of pre-period (tail). The devices can be used as building blocks when constructing of unpredictable PRNG.

Peer-review under responsibility of the scientific committee of the 8th Annual International Conference on Biologically Inspired Cognitive Architectures

Keywords: Pseudorandom Number Generator, NLFSR, Universal NLFSR, Tail.

1 Introduction

The article is devoted to a pseudorandom number generator (PRNG) aimed at using in tasks of information protection (IP) from accidental and deliberate destructive influences. In other words, these are generators with strict requirements for unpredictability and statistical security of generated sequences. The principles of designing non-binary PRNGs on non-linear feedback shift registers (NLFSRs) are considered. The main advantages of the PRNG of this type are the simplicity of software and hardware implementation, high speed and good statistical properties.

2 Stochastic methods of information protection

Analysis of threats to cybersecurity and widespread use of vulnerable supercomputer, mobile, cyberphysical and RFID (radio frequency identification) technologies allows us to conclude that the

Peer-review under responsibility of the scientific committee of the 8th Annual International Conference on Biologically Inspired Cognitive Architectures
10.1016/j.procs.2018.01.032

role of stochastic IP methods is constantly increasing (Osmolovskij 1991, 2003; Ivanov 2012). Stochastic methods are usually called the methods, directly or indirectly based on the use of unpredictable PRNGs. With the use of the PRNG, almost all of the IP tasks are successfully solved. In some cases, stochastic methods are the only possible mechanism for protecting information from an active adversary. A special case of stochastic methods is the cryptographic methods of the IP.

The process of information hashing can be considered as an overlay of a pseudorandom sequence (PRS) on the input information sequence. This seemingly controversial statement became evident after the appearance of the new SPONGE hash construction (Bertoni 2016).

The effectiveness of protection when using stochastic methods is determined by the quality of the algorithms used, respectively, the PRS generation and hashing.

As an example of the universal stochastic IP method, one can mention the method of introducing unpredictability in the work of means and objects of protection (the method of randomization). Its implementation in principle cannot be imagined without the use of the PRNG. It can be used in conjunction with any other method of protection, automatically increasing its quality. In this case, unpredictability can be inserted not only into the sequence, time of execution of individual acts of the algorithm or the mechanism of the functioning of the software, but also even into the result of the algorithm work. The methods of program obfuscating and the methods of protecting software from unauthorized use also require the use of the PRNG. The use of randomization in the design of digital equipment makes it possible to protect it from leakage of information through side channels. Examples of the PRNG use and hash generators in IP protection tasks can be found in (Osmolovskij 1991, Ivanov 2012, Goldreich, 2010, Bellare 1994, 1997; Goldwasser 1984, RSAES-OAEP 2000, Boeck 2016).

Thus, we can draw a conclusion about the determining role of the qualitative PRNGs in the IP systems. For example, in the presence of the unpredictable PRNGs all other symmetric cryptography primitives can be efficiently built. It should be remembered that stochastic methods of the IP are classical dual-use methods, as they are used not only for solving the IP issues, but also for attacks on computer systems, which have been successfully demonstrated for a long time by the creators of permutation, polymorphic and metamorphic malicious programs (Razrushayushchie 2011).

3 PRNG on non-linear feedback shift register

In (Ivanov 2012, the principles of designing binary and non-binary PRNG on linear feedback shift registers (LFSR) were considered. This article focuses on the PRNG on non-linear feedback shift registers (NLFSR).

The general scheme of the NLFSR is shown in Fig. 1, where Q_1, Q_2, ..., Q_N are generator registers, F is a non-linear function of the Fibonacci generator, F_1, F_2, ..., F_N are linear or non-linear functions of the Galois generator (Dubrova 2008). In the case of the Galois generator, at least one of the functions F_i is non-linear. Like the LFSR, the NLFSR can be used as elementary building blocks in the construction of the unpredictable PRNG (in some cases, with greater cryptographic robustness than the LFSR) and they serve as the basis for stream ciphers. Moreover, their main advantage is high efficiency in hardware implementation. The most revealing example on this topic is the PRNG of the Trivium stream cipher (Canniere 2008). The main problem in the synthesis of the PRNG based on the NLFSR is to provide a large period of generated sequences. In (Dubrova 2012a, 2011, 2012b, 2008, 2014; Chabloz 2010, Mansouri) the questions of constructing binary NLFSRs with a guaranteed longer period are considered. This paper focuses solely on the non-binary NLFSRs.