Chaotic Keystream Generator Using Coupled NDFs with Parameter Perturbing

Xiaomin Wang[1], Jiashu Zhang[1], and Wenfang Zhang[2]

[1] Sichuan Province Key Lab of Signal and Information Processing,
Southwest Jiaotong University, Chengdu 610031, P.R. China
hornwong@hotmail.com, jszhang@home.swjtu.edu.cn
[2] School of Information Science and Technology,
Southwest Jiaotong University, Chengdu 610031, P.R. China
wfzhang2001@163.com

Abstract. Chaotic cryptology has been widely investigated recently. This paper analyzes the security pitfalls existing in digital chaotic stream ciphers, which work on the well characterized one-dimensional(1-D) chaotic systems. As a practical solution to these problems caused by 1-D chaotic systems, a chaotic keystream generator using nonlinear digital filters with n-D uniform distribution is proposed. To improve system security further and overcome the effects of finite wordlength, the coupling method with parameter perturbing is considered. Detailed theoretical analyses show that it has perfect cryptographic properties, and can be used to construct stream ciphers with higher security than other 1-D chaotic ciphers. Finally, some numeric experiments are made and the experimental results coincide well with the theoretical analyses.

Keywords: Chaos, Cryptology, Keystream, Nonlinear digital filter.

1 Introduction

In recent years, chaotic cryptography has received considerable attention. Both digital and analog chaotic encryption methods have been proposed and analyzed [13, 12, 14, 5, 1, 16, 36, 15, 33, 4, 17, 30, 27, 3, 2]. The main advantage using chaos lies in the observation that a chaotic signal looks like noise for the unauthorized users. Secondly, some interesting properties, such as mixing and sensitivity to initial conditions, can be connected with those of good ciphers, such as confusion and diffusion [13, 12, 14, 5, 1, 24]. Moreover, generating chaotic signal is often of low cost with simple iterations, which makes it suitable for the construction of stream ciphers.

Generally speaking, chaotic stream ciphers use chaotic systems to generate pseudorandom keystream to encrypt the plaintext one by one. Many different chaotic systems have been utilized to generate such keystreams, 2-D Hénon attractor in [2], generalized logistic map in [1], piecewise linear chaotic map

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 270–285, 2006.

(PWLCM) in [30,3,4,31]. In [6] multiple chaotic system are used, and in [14,11] coupled PWLCMs and coupled map lattices are employed irrespectively. The keystreams are then generated from the outputs of underlying chaotic systems by different post-processing methods, e.g., extracting some bits from chaotic orbits [1,30,6], determining by which interval the chaotic orbits reach [3,2,32], cascading multiple chaotic systems [8], and coupling chaotic systems [14, 11]. Except the algorithms in [14, 11], unfortunately, several keystream algorithms have been known not secure enough [20,9,21,22].

Why so many chaotic keystream algorithms are not secure? The reasons may lie in at least two aspects. One is bad properties of the underlying chaotic systems, i.e, too small key space to resist brute-force attack; irregular attractor regions with periodic windows to hardly select robust keys. The other factor is the improper construction of the output keystreams. For example, the keystreams directly outputting from the chaotic orbit of a single chaotic system, may suffer from the phase space reconstruction or return map attack [26]; the keystreams coming from the symbols ,which have fixed relation with intervals the orbit reaching, will leak some secret information to the opponent, and may be susceptible to the nonlinear forecasting attack [25]; the keys with non-equally strong or the key space not a product but a summation of all the parameters involved, will be compromised under the error function attack (EFA) [28]. Besides the above reasons, other factors such as finite realization precision, parameter sensitivity, ergodicity, etc., have not been considered carefully. For detailed discussions please see [20].

Most digital chaotic stream ciphers and pseudorandom number generators, to our best knowledge, employ the 1-D chaotic maps(e.g. logistic map,tent map, Bernoulli map, PWLCM, etc.) due to their well characterized from a theoretical point of view and simple electronic implementation. These maps, however, only preserve 1-D uniform distribution, which result that any successive points in chaotic orbit are not independent each other. Thus the unpredictability of pseudorandom sequence is decreased. The common and efficient approach is of under-sampling, i.e. only sample one point during every n iterations, to eliminate such correlation. Unfortunately, this way reduces the generator speed inevitably, worst case n times. So signals with not only 1-D but n-D uniform distribution are required for chaotic keystream generators(CKGs).

This paper investigates some fascinating properties of nonlinear digital filter(NDF),such as ergodicity and n-dimensional uniform distribution, and then a NDF-based chaotic keystream generator(NDF-CKG) is presented. Different from the existing CKGs, the proposed scheme works on the chaotic systems with n-dimensional uniform distribution. To overcome the effects of finite computing precision, a coupling method with parameter perturbing is utilized. Theoretical analyses and experiments show that the proposed NDF-CKG has perfect cryptographic properties. Benefiting from the inherent parallel structure of filter, furthermore, the NDF-CKG is suitable for software realization with parallel algorithm or digital circuit implementation.