Chapter 34
Design of a Chaotic Random Bit Generator Using a Duffing – van der Pol System

Christos Volos
Aristotle University of Thessaloniki, Greece

Ioannis Stouboulos
Aristotle University of Thessaloniki, Greece

Ioannis Kyprianidis
Aristotle University of Thessaloniki, Greece

Sundarapandian Vaidyanathan
Vel Tech University, India

ABSTRACT

In this paper a chaotic random bit generator, which is based in one of the most well-known non-autonomous chaotic dynamical systems, the Duffing van der Pol, is presented. The basic component of this design approach is the use of the Poincaré map of the aforementioned system. The produced chaotic attractor of the Duffing van der Pol system is converted with the proposed method to a random bit sequence. Furthermore, for, improving the "randomness" of the produced bit streams the X-OR function in the outputs of two threshold circuits that use two variables x which are produced by the two Duffing – van der Pol's Poincaré maps is used. Finally, the produced bit sequence is subjected to the de-skewing technique to extract unbiased bits with no correlation and so to increase their complexity, as it is confirmed by the statistical test suite, FIPS-140-2.

1. INTRODUCTION

In the last decades, the information security depends upon the generation of unpredictable quantities, such as the keystream in the one-time pad, the secret key in the DES encryption algorithm, the primes p, q in the RSA encryption and digital signature schemes, the private key a in the DSA, and the challenges used in challenge-response identification systems. In all these cases, the generated quantities must be of sufficient size and mainly must be "random" in the sense that the probability of any particular value being selected must be sufficiently small to preclude an adversary from gaining advantage through optimizing a search strategy based on such probability.

DOI: 10.4018/978-1-5225-1759-7.ch034

This is the reason why the last decades many research teams tried to design devices or algorithms which output sequences of statistically independent and unbiased binary digits. These devices or algorithms are called Random Bit Generators (RBGs). Many RBGs have been proposed so far. All these can be classified, based on the source of the randomness, into three major types: True Random Bit Generators (TRBGs), Pseudo-Random Bit Generators (PRBGs) and Hybrid Random Bit Generators (HRBGs) (Shu, 1995).

The first type, the TRBGs, require a naturally occurring source of randomness, which comes from an unpredictable natural process in a physical or hardware device, as it has been reported till now (Agnew, 1986; Bardis et al., 2009; Davis et al., 1994; Dube, 2008; Fairfield et al., 1987; Guide, 1985; Holman et al., 1997; Hu et al., 2009; Trcek, 2006). However, the design of a hardware device for exploiting the randomness and producing a bit sequence, which will be free of biases and correlations, is a very difficult task.

To overcome this difficulty many research teams have proposed the development of PRBGs, which are deterministic algorithms that output a random binary sequence (Blum et al., 1986; Ferguson & Schneier, 2003; Knuth, 1981; Matsumoto & Nishimura, 1997; Menezes et al., 1996; Park & Miller, 1988). This bit sequence is not truly random in that it is completely determined by a relatively small set of initial values (seed). PRBGs are very important in practice for their speed in number generation, their portability and their reproducibility, and they are thus central in applications such as simulations, e.g., of physical systems with the Monte Carlo method, in cryptography, and in procedural generation. However, in PRNGs due to the fact that the output is a function of the input, the actual entropy of the output can never exceed the entropy of the input. Hence, the randomness level of the pseudo-random numbers depends on the level of randomness of the input.

Thus, HRNGs have been proposed to use a random generator as a "seed" generator and expand it. A seed generator is a hardware-based RNG with or without user's interaction, such as mouse movements, random keystrokes, or hard drives seek times (Koc, 2009).

Furthermore, in the last two decades, chaotic dynamical systems (Hasselblatt & Katok, 2003; Vaidyanathan & Azar, 2015a, b, c, d, e), have aroused tremendous interest, not only of their applications in several disciplines including physical and social sciences (Grebogi & Yorke, 1997), as well as their potential use in various control and synchronization schemes (Azar & Vaidyanathan, 2015a, b, c, d; Vaidyanathan et al., 2015a, b, c, d; Zhu & Azar, 2015; Azar & Zhu, 2015), but also of their structural relationship with cryptographic systems, as it is shown in Table 1 (Alvarez & Li, 2006).

Table 1. Properties of cryptographic systems and their analogous properties of chaotic systems

Cryptographic Systems	Chaotic Systems
Confusion	Ergodicity
Diffusion with small changes in plaintext / secret keys	Sensitivity to initial conditions / system parameters
Diffusion with a small change within one block of the plaintext	Mixing property
Deterministic pseudo randomness	Deterministic dynamics
Algorithmic complexity	Structural complexity