Generation of cryptographic sequences by means of difference equations

Amparo Fúster Sabater

Security Information Institute, C.S.I.C.
144 Serrano, 28006 Madrid, Spain

amparo@iec.csic.es

Extended Abstract

Pseudorandom binary sequences are typically used in a wide variety of applications such as: spread spectrum communication systems, multiterminal system identification, global positioning systems, software testing, error-correcting codes or cryptography (stream ciphers). This work deals specifically with this last application.

Symmetric key encryption functions are usually divided into two separated classes: stream ciphers and block-ciphers depending on whether the encryption function is applied either to each individual bit or to a block of bits of the plaintext, respectively. Stream ciphers are the fastest among the encryption procedures so they are implemented in many technological applications e.g. RC4 for encrypting Internet traffic [13] or the encryption function E0 in Bluetooth specifications [1]. Stream ciphers try to imitate the mythic *one-time pad cipher* or *Vernam cipher* [11] and are designed to generate a long sequence (the *keystream sequence*) of pseudorandom bits. Some of the most recent designs in stream ciphers can be found in [4], [14]. This keystream sequence is XORed with the plaintext (in emission) in order to obtain the ciphertext or with the ciphertext (in reception) in order to recover the plaintext.

Most keystream generators are based on maximal-length Linear Feedback Shift Registers (LFSRs) [8] whose output sequences, the so-called PN-sequences, are combined in a non linear way (by means of non linear filters, non linear combinators or irregularly decimated generators) in order to produce pseudorandom sequences of cryptographic application [6], [7], [11].

Inside the family of irregularly decimated generators, we can enumerate: a) the *shrinking generator* proposed by Coppersmith, Krawczyk and Mansour [2] that includes two LFSRs, b) the *self-shrinking generator* designed by Meier and Staffelbach [10] involving only one LFSR and c) the *generalized self-shrinking generator* proposed by Hu and Xiao [9] that includes the self-shrinking generator. Irregularly decimated generators produce good cryptographic sequences ([5], [11], [12], [3]) characterized by long periods, good correlation features, excellent run distribution, balancedness, simplicity of implementation, etc. The underlying idea of this kind of generators is the irregular decimation of an PN-sequence according to the bits of another one. The decimation result is the output sequence that will be used as keystream sequence in the cryptographic procedure.

In this work, it is shown that the sequences generated by these decimation generators are particular solutions of binary coefficient homogeneous linear difference equations. In fact, all these sequences are just linear combinations of primary sequences weighted by binary coefficients. Cryptographic parameters of such sequences (e.g. period, linear complexity, balancedness) can be analyzed in terms of linear equation solutions. It must be noticed that, although these sequences are irregularly decimated, in practice they are simple solutions of linear equations. This fact establishes a subtle link between irregular decimation and linearity that can be conveniently exploited in the cryptanalysis of such keystream generators.

At the same time, other solution sequences not included in the previous families also exhibit good properties for their application in cryptography. In brief, computing the solutions of linear difference equations provides one with new binary sequences whose cryptographic parameters can be easily guaranteed. That is to say, linear difference equations can contribute very efficiently to the generation of keystream sequences for stream cipher.

Bibliography

[1] Bluetooth, *Specifications of the Bluetooth system,* Version 1.1, available at http://www.bluetooth.com/

[2] D. Coppersmith, H. Krawczyk and Y. Mansour, The Shrinking Generator. Proc. of CRYPTO'93. LNCS, Springer Verlag, Vol. 773, pp. 22-39, 1994.

[3] Diehard Test: Test suite for random numbers, available at http://stat.fsu.edu./pub/diehard/

[4] eSTREAM, the ECRYPT Stream Cipher Project, Call for Primitives, available at http://www.ecrypt.eu.org/stream/

[5] A. Fúster-Sabater and P. Caballero-Gil, Strategic Attack on the Shrinking Generator, Theoretical Computer Science, Vol. 409, No. 3, pp. 530-536, 2008.

[6] A. Fúster-Sabater, P. Caballero-Gil and O. Delgado-Mohatar, Deterministic Computation of Pseudorandomness in Sequences of Cryptographic Application. Proc. of ICCS 2009, Part I, LNCS, Springer-Verlag, Vol. 5544, pp. 621-630, 2009.

[7] A. Fúster-Sabater and P. Caballero-Gil, Chaotic modelling of the generalized self-shrinking generator, Appl. Soft Comput., Vol. 11, pp. 1876-1880, 2011.

[8] S.W. Golomb, Shift Register-Sequences, Aegean Park Press, Laguna Hill, 1982.

[9] Y. Hu and G. Xiao, Generalized Self-Shrinking Generator, IEEE Trans. Inform. Theory, Vol. 50, pp. 714-719, April 2004.

[10] W. Meier and O. Staffelbach, The Self-Shrinking Generator, in Proc. EUROCRYPT'94. LNCS, Springer Verlag, Vol. 950, pp. 205-214, 1995.

[11] A.J. Menezes *et al.*, Handbook of Applied Cryptography, New York:CRC Press, 1997.

[12] NIST SP 800-20 Rev. 1a: Test suite for random numbers, available at http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf

[13] G. Paul and S. Maitra, RC4 Stream Cipher and Its Variants, Discrete Mathematics and Its Applications, CRC Press, Taylor & Francis Group, Boca Raton, FL, 2012.

[14] Robshaw M, Billet O. New Stream Cipher Designs: The eSTREAM Finalist. Lecture Notes in Computer Science, vol. 4986. Berlin, Germany: Springer-Verlag 2008.