CRYPTANALYSIS OF THE SELF-SHRINKING GENERATOR

Milan Vojvoda

Department of Mathematics, Faculty of Electrical Engineering and Information Technology
Slovak University of Technology
Ilkovičova 3, 812 19 Bratislava, Slovak Republic
vojvoda@kmat.elf.stuba.sk

The design goal in stream ciphers is to efficiently produce pseudorandom sequences - keystreams (i.e. sequences that possess properties common to truly random sequences and in some sense are "indistinguishable" from these sequences) [2], [5]. The self-shrinking generator [3] is one of the many proposed and studied keystream generators. It is based on the shrinking principle [1], has low hardware requirements but produces the keystream bits irregularly. The known plaintext attacks against the self-shrinking generator were presented in [4], and [6].

In our contribution we study the security of the self-shrinking generator when used as a generator of short random strings (challenges). The challenge generators are used e.g. in GSM and UMTS networks. The user sends to the network the authentication request and the network responds sending the user the generated challenge. The user computes then its answer to the received challenge and sends this answer back to the network. Hence the challenge (keystream) is known and moreover it is possible to measure the response time of the network (time between sending the authentication request and receiving the challenge). In this contribution we study the influence of the known response time on the known plaintext attack against the self-shrinking generator.

This research was supported by VEGA-grant 1/7611/20.

References

[1] Coppersmith, D., Krawczyk, H., Mansour, Y.: *The shrinking generator*, Advances in Cryptology - EUROCRYPT '93, vol. 773 of LNCS, Springer-Verlag 1993, pp. 22-39.

[2] Grošek, O.: *On the stability of stream ciphers (O stabilite prúdových šifier)*, Abstracts of the conference "Jesenný seminár z kryptoanalýzy", L.Mikuláš, October 9-11, 1996, pp.14-26, (in Slovak).

[3] Meier, W., Staffelbach, O.: *The self-shrinking generator*, Advances in Cryptology - EUROCRYPT '94, vol. 950 of LNCS, Springer-Verlag 1995, pp. 205-214.

[4] Mihaljević, M.J.: *A faster cryptanalysis of the self-shrinking generator*, Advances in Cryptology - ACISP '96, vol. 1172 of LNCS, Springer-Verlag 1996, pp. 182-189.

[5] Nemoga, K.: *Linear recurring sequences (Lineárne rekurentné postupnosti)*, Abstracts of the conference "Jesenný seminár z kryptoanalýzy", L.Mikuláš, October 9-11, 1996, pp.1-13, (in Slovak).

[6] Zenner, E., Krause, M., Lucks, S.: *Improved cryptanalysis of the self-shrinking generator*, Advances in Cryptology - ACISP '2001, vol. 2119 of LNCS, Springer-Verlag 2001, pp. 21-35.