LPV dynamical systems and Self-Synchronizing Stream Ciphers: Stanislas and further

Hamid Boukerrou[1] Marine Minier[2] Gilles Millerioux[1]

[1]Université de Lorraine, CNRS, CRAN, UMR 7039, France, email: {hamid.boukerrou,gilles.millerioux}@univ-lorraine.fr

[2]Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France, email: marine.minier@loria.fr

Abstract

Self-Synchronizing Stream Ciphers (SSSCs) were patented in 1946. The basic principle of such ciphers is to encrypt every plaintext symbol with a transformation that only involves a fixed number of previous ciphertext symbols. Therefore, every ciphertext symbol is correctly deciphered provided that previous symbols have been properly received. This self-synchronization property has many advantages and is especially relevant to group communications. In this respect, since 1960, specific SSSCs have been designed and are still used to provide bulk encryption (for Hertzian line, RNIS link, etc.) in military applications or governmental radio mobile networks [Mau91], [Rue12]. The canonical form of the SSSC combines a shift register, which acts as a state register with the ciphertext as input, together with a filtering function that provides the running key stream. The cryptographic complexity of the canonical form of the SSSC lies in the filtering function. In the early 90s, studies have been performed [Mau91], [DGV92] to propose secure designs of SSSCs. These works have been followed by effective constructions ([PHM04], [Sar03], [DK08]). Following Maurer's work, some constructions have been proposed ([JM03], [JM05], [JM06], [KRB$^+$08]) but have all been broken by cryptanalysis work in ([Kli05], [Dwo01], [VY02], [ABMP11], [DGM17]). However, there is a common point to all these constructions, it is that they involve automata using triangular state transition functions "T-function" [KS04].

In [FBH$^+$20], a methodology borrowed from graph and control theory has been proposed to construct a family of SSSC admitting non-triangular state transition functions. This family involves so-called Linear Parameter Varying (LPV) automata described by matrix equations and having the property of flatness. An instantiation, called Stanislas, is proposed with a proof of security. Flatness is a specific property of dynamical systems that guarantees in this context the construction of automata with finite input memory and thus self-synchronization.

Then, an improvement has been proposed in [BMM21] to enhance the diffusion property regarding the security. To this end, an hybrid architecture with two modes of operations is introduced, each one governed by an LPV model that switches one another. The architecture is motivated to take advantage of both properties namely self-synchronization and good diffusion. It is shown that the resulting cipher is a statistical SSSC.

Finally, as an extension, a hybrid architecture for Multiple Input Multiple Output (MIMO) LPV systems is under investigation to accelerate the encryption process. Indeed, instead of constructing Single Input Single Output (SISO) LPV systems that are used to perform symbol-by-symbol encryption, MIMO LPV systems are sough to allow encrypting several symbols at a time.

References

[ABMP11] François Arnault, Thierry Berger, Marine Minier, and Benjamin Pousse. Revisiting lfsrs for cryptographic applications. *IEEE Transactions on Information Theory*, 57(12):8095–8113, 2011.

[BMM21] Hamid Boukerrou, Gilles Millérioux, and Marine Minier. Hybrid architecture of lpv dynamical systems in the context of cybersecurity. *IFAC-PapersOnLine*, 54(8):154–161, 2021.

[DGM17] Brandon Dravie, Philippe Guillot, and Gilles Millérioux. Design of self-synchronizing stream ciphers: A new control-theoretical paradigm. In *20th IFAC World Congress, IFAC 2017*, Toulouse, France, July 2017.

[DGV92] J. Daemen, R. Govaerts, and J. Vandewalle. On the design of high speed self-synchronizing stream ciphers. In *[Proceedings] Singapore ICCS/ISITA '92*, pages 279–283 vol.1, 1992.

[DK08] Joan Daemen and Paris Kitsos. *The Self-synchronizing Stream Cipher Moustique*, volume 4986, pages 210–223. 06 2008.

[Dwo01] Morris J Dworkin. Sp 800-38a 2001 edition. recommendation for block cipher modes of operation: Methods and techniques, 2001.

[FBH+20] Julien Francq, Loic Besson, Paul Huynh, Philippe Guillot, Gilles Millerioux, and Marine Minier. Non-triangular self-synchronizing stream ciphers. *IEEE Transactions on Computers*, 2020.

[JM03] Antoine Joux and Frédéric Muller. Loosening the knot. In *FSE*, 2003.

[JM05] Antoine Joux and Frédéric Muller. Two attacks against the hbb stream cipher. volume 3557, pages 330–341, 02 2005.

[JM06] Antoine Joux and Frédéric Muller. Chosen-ciphertext attacks against mosquito. In *International Workshop on Fast Software Encryption*, pages 390–404. Springer, 2006.

[Kli05] Vlastimil Klima. Cryptanalysis of hiji-bij-bij (hbb), 2005. v.klima (at) volny.cz 12788 received 5 Jan 2005.

[KRB+08] Emilia Käsper, Vincent Rijmen, Tor E. Bjørstad, Christian Rechberger, Matt Robshaw, and Gautham Sekar. Correlated keystreams in moustique. In Serge Vaudenay, editor, *Progress in Cryptology – AFRICACRYPT 2008*, pages 246–257, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[KS04] Alexander Klimov and Adi Shamir. New cryptographic primitives based on multiword t-functions. In *International Workshop on Fast Software Encryption*, pages 1–15. Springer, 2004.

[Mau91] Ueli M. Maurer. New approaches to the design of self-synchronizing stream ciphers. In Donald W. Davies, editor, *Advances in Cryptology — EUROCRYPT '91*, pages 458–471, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.

[PHM04] G. G. Rose P. Hawkes, M. Paddon and W. V. Miriam. Primitive specification for sss. *e-Stream Project*, Tech. Rep., 2004.

[Rue12] Rainer A Rueppel. *Analysis and design of stream ciphers*. Springer Science & Business Media, 2012.

[Sar03] Palash Sarkar. Hiji-bij-bij: A new stream cipher with a self-synchronizing mode of operation. volume 2904, pages 36–51, 03 2003.

[VY02] Serge Vaudenay and Amr M Youssef. *Selected Areas in Cryptography*. Springer, 2002.