New LFSRs and FCSRs representations for stream ciphers hardware and software design

François Arnault[1], Thierry Berger[1], Cédric Lauradoux[2], Marine Minier[2] and Benjamin Pousse[1]

[1] XLIM (UMR CNRS 6172), Université de Limoges
23 avenue Albert Thomas, F-87060 Limoges Cedex - France
first name.name@xlim.fr
[2] Lyon University - CITI Laboratory / SWING INRIA team
6, avenue des arts - 69621 Villeurbanne Cedex - France
first name.name@inrialpes.fr

Abstract. In this talk, we will sum up our recent research results concerning the introduction of a new representation for FCSRs based upon a known LFSRs representation. This matrix based representation allows to construct FCSRs with a more compact hardware representation and a quicker diffusion while preserving the usual and proven good properties (good periods, ℓ-sequences, good statistical behaviors, etc.). Moreover, this new approach circumvents the weaknesses of the Fibonacci and Galois representations described in [3] and in [4]. We also show how to extend the LFSRs representation to a particular LFSR case called the windmill case.

LFSRs are well-known primitives used in cryptography especially for stream cipher design. However they have some drawbacks when looking at their resistance against algebraic attacks because of their linearity. In the contrary, FCSRs are inherently resistant to algebraic attacks due to the non-linearity of the update function. Using the new representation, we propose two new stream ciphers based on the so-called "ring" FCSR representation. The first proposal called F-FCSR (see [1]) is dedicated to hardware applications whereas the second proposal called X-FCSR (see [2]) is designed for software purposes but is also efficient in hardware.

Keywords: Stream ciphers, LFSRs, FCSRs, windmill representations.

References

1. François Arnault, Thierry P. Berger, Cédric Lauradoux, Marine Minier, and Benjamin Pousse. A new approach for fcsrs. In *Selected Areas in Cryptography, 16th Annual International Workshop, SAC 2009*, volume 5867 of *Lecture Notes in Computer Science*, pages 433–448. Springer, 2009.
2. Thierry P. Berger, Marine Minier, and Benjamin Pousse. Software oriented stream ciphers based upon fcsrs in diversified mode. In *INDOCRYPT 2009, 10th International Conference on Cryptology in India*, volume 5922 of *Lecture Notes in Computer Science*, pages 119–135. Springer, 2009.

3. Simon Fischer, Willi Meier, and Dirk Stegemann. Equivalent Representations of the F-FCSR Keystream Generator. In *ECRYPT Network of Excellence - SASC Workshop*, pages 87–94, 2008. Available at http://www.ecrypt.eu.org/stvl/sasc2008/.
4. Martin Hell and Thomas Johansson. Breaking the f-fcsr-h stream cipher in real time. In *Advances in Cryptology - ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security*, volume 5350 of *Lecture Notes in Computer Science*, pages 557–569. Springer, 2008.