Abstract. The F-FCSR stream cipher family has been presented a few years ago. Apart from some flaws in the initial propositions, corrected in a later stage, there are no known weaknesses of the core of these algorithms. Two variants, F-FCSR-H and F-FCSR-16, were proposed in the eSTREAM project, and F-FCSR-H v2 is one of the ciphers selected for the eSTREAM portfolio.

In this paper we present a new and severe cryptanalytic attack on the F-FCSR stream cipher family. We give the details of the attack when applied to F-FCSR-H v2 and F-FCSR-16. The attack requires a few Mbytes of received sequence, and the complexity is low enough to allow the attack to be performed on a single PC within seconds.

Key words. Stream cipher, Cryptanalysis, F-FCSR-H, F-FCSR-16, Linearization.

1. Introduction

The cryptographic scene includes a variety of efficient and trusted block ciphers. However the same does not seem to hold for stream ciphers. The stream ciphers that have received attention through use in various standards tend to have more or less serious security weaknesses. Examples are A5 algorithms used in GSM, the RC4 algorithm used in, for example, WLAN applications through the WEP protocol, and the E0 stream cipher used in Bluetooth.

Based on a belief that a dedicated stream cipher still has a capability of significantly outperforming a block cipher, the eSTREAM project was launched in 2004. The goal of this project was to solicit and evaluate submitted proposals of stream ciphers for future standardization. The main evaluation criteria set up were long-term security, efficiency in terms of performance, flexibility, and market requirements. The eSTREAM project was not a standardization body, like the AES project or the ongoing SHA-3 project. The

* This paper was solicited by the Editors-in-Chief as one of the best papers from Asiacrypt 2008, based on the recommendation of the program committee.
goal was to stimulate work in the area of stream ciphers. As an example, designers were allowed to tweak their proposals in the early phases of the project.

The eSTREAM project considered two different profiles, one targeting software implemented stream ciphers, profile 1; and one for hardware implemented stream ciphers (in particular constrained devices), profile 2. The hardware category received a total of 25 submitted proposals. After three phases of evaluation, the final eSTREAM portfolio recommended four of them. One of them is a design called F-FCSR-H v2.

F-FCSR-H v2 is one of several algorithms in the F-FCSR family of stream ciphers designed by F. Arnault, T.P. Berger, and C. Lauradoux. The family of ciphers is based on feedback with carry shift registers (FCSR) together with a filtering function. The idea of using FCSRs to generate sequences for cryptographic applications was initially proposed by Klapper and Goresky in [21]. The F-FCSR family was introduced in [2], proposing four concrete constructions. These proposals were cryptanalyzed in [19]. The initial version submitted to eSTREAM, targeting hardware, was called F-FCSR-H. It was shown in [18] that this construction also had security problems. This led to a change in the initialization procedure, and the resulting algorithm was named F-FCSR-H v2. Also, a new variant called F-FCSR-16 was proposed. This variant outputs 16 bits in each register update compared to 8 bits in F-FCSR-H v2. This paper will focus on the specification of F-FCSR-H v2 and F-FCSR-16 given in [6]. A more comprehensive overview of stream ciphers based on FCSRs is given in Appendix A.

The eSTREAM class of hardware stream ciphers (and F-FCSR-H v2 in particular) prescribes a key of length 80 bits. F-FSCR-16 can be used with either 80 or 128 bit key, with the 80 bit choice targeting profile 2 (hardware) and the 128 bit choice targeting profile 1 (software) in eSTREAM. The constructions also use a public IV value of bit-size $v$ which can be set in the interval $32 \leq v \leq 80$ for F-FCSR-H v2 and $32 \leq v \leq 128$ for F-FCSR-16.

Apart from exhaustive key search, there are a number of standard attacks that can be applied. Time-memory-data trade-off attacks of different kinds [10,13,16] are applicable, but due to fairly large state size (size of the FCSR), this does not give a successful attack. Correlation attacks and linear cryptanalysis techniques [25,26] are also possible approaches, but the nonlinearity of the carry in the FCSR makes this difficult, and no promising ideas in this direction have been proposed. Also algebraic attacks has been accounted for in the design. Another standard technique today is a chosen IV attack [14,27,29], but the latest versions of the F-FCSR have not shown weaknesses in the initialization. So apart from the initial flaws (on the IV-setup procedure, and a TMD tradeoff attack), there were no known weaknesses of the core of these algorithms until a preliminary version of this paper was presented in [17].

We present a new and severe cryptanalytic attack on the F-FCSR stream cipher family. We give the details of the attack when applied to F-FCSR-H v2. The attack is based on observing that the contribution of nonlinearity comes from the carry bits only and that sometimes this contribution is too low and the system can be linearized. We define this as an *event*, and when the event occurs, we show how we can very efficiently derive the whole state. The whole attack requires a few Mbytes of received sequence, and the complexity is low enough to allow the attack to be performed on a single PC within seconds. The attack has been fully implemented using the designers’ reference implementation. Simulations show that the attack requires $2^{24.7}$ keystream bytes for F-FCSR-H v2 and $2^{21.5}$ keystream bytes for F-FCSR-16.