Improved Fast Correlation Attack on the Shrinking and Self-shrinking Generators*

Kitae Jeong[1], Jaechul Sung[2], Seokhie Hong[1], Sangjin Lee[1], Jaeheon Kim[3], and Deukjo Hong[1]

[1] Center for Information Security Technologies (CIST), Korea University, Seoul, Korea
{kite,hsh,sangjin,hongdj}@cist.korea.ac.kr
[2] Department of Mathematics, University of Seoul, Seoul, Korea
jcsung@uos.ac.kr
[3] National Security Research Institute (NSRI), 161 Gajeong-dong, Yuseong-gu, Daejeon 305-350, Korea
jaeheon@etri.re.kr

Abstract. The fast correlation attack on the shrinking generator proposed by Zhang et al. in [8] has a room for improvement that the probability that the guessing bit is incorrect increases in certain case. In this paper, we propose a method to improve Zhang et al.'s attack. Reflecting our idea, the fast correlation attack on the shrinking and self-shrinking generator is more efficient than Zhang et al.'s attack in both data and computational complexities. For the shrinking generator, required keystream bits and computational complexity are reduced about 69% and 27%, respectively; For the self-shrinking generator, required keystream bits and computational complexity are reduced about 46% and 22%, respectively.

Keywords: Clock-controlled generator, Shrinking generator, Self-Shrinking generator, Fast correlation attack.

1 Introduction

The shrinking generator is a clock-controlled generator proposed in [3]. It consists of the generating LFSR and the control LFSR. Both LFSRs are clocked regularly and simultaneously. If a current output bit of the control LFSR is 1, then the corresponding output bit of the generating LFSR is taken as a keystream bit. Otherwise it is discarded. In [8], Zhang et al. showed that a fast correlation attack can be applied to the shrinking generator. They guess the sequence of the generating LFSR by computing the probability that an output bit of the generating LFSR appears in a particular interval of keystream bits and then

* "This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)" (IITA-2006-(C1090-0603-0025)).

P.Q. Nguyen (Ed.): VIETCRYPT 2006, LNCS 4341, pp. 260–270, 2006.

recover the initial state of the generating LFSR by applying the fast correlation attack proposed by Chose et al. in [1]. So far, the most efficient attack on the shrinking generator is Zhang et al.'s attack.

The main idea in their guessing the sequence of the generating LFSR is to choose the major bit value between 0 and 1 in an intended interval of the keystream bits. However, their method has a room for improvement that the probability that the guessing bit is incorrect increases as the difference between the number of the 0 bits and 1 bits becomes small.

In this paper, we propose a method to improve Zhang et al.'s attack. We set a threshold of the difference between the number of the 0 bits and 1 bits, and reduce the error probability by guessing the sequence of the generating LFSR only in the interval where the difference between the number of the 0 bits and 1 bits is greater than the threshold. Reflecting our idea, our attack on the shrinking generator is more efficient than Zhang et al.'s attack in both data and computational complexities. The reason is as follows. In the first place, Zhang et al. only consider an interval that includes odd number of integers. We only consider an interval where the difference between the number of the 0 bits and 1 bits is greater than the threshold. Because Zhang et al.'s attack and our attack use refined intervals, the length of the guessed sequence is almost same in two attacks. Secondly, the probability that the guessing bit is correct in our attack is larger than that in Zhang et al.'s attack. So the correlation in our attack is larger than that in Zhang et al.'s attack. Hence our attack is more efficient than Zhang et al.'s attack. Table 1 shows the comparison of Zhang et al.'s attack and our attack on the shrinking generator (the length of the generating LFSR and the control LFSR is respectively 61 and 60) with success probability 99.9%. Zhang et al.'s attack requires $2^{17.1}$ keystream bits and computational complexity of $2^{56.7786}$; Our attack requires $2^{15.43}$ keystream bits and computational complexity of $2^{56.3314}$. In our attack, required keystream bits and computational complexity are reduced about 69% and 27%, respectively.

We also show that our attack works well on the self-shrinking generator. The self-shrinking generator is a modified version of the shrinking generator which is proposed by Meier and Staffelbach in [5]. It requires a single LFSR, whose length will be denoted by L. The selection rule is the same as for the shrinking generator, using even bits as output sequences generated by the control LFSR and odd bits as output sequences generated by the generating LFSR. Thus the selection rule of self-shrinking generator requires a tuple (even bit, odd bit) as input and outputs a odd bit if and only if a even bit is 1. In [5], the initial state of the generator from a short keystream sequence is reconstructed requiring $\mathcal{O}(2^{0.75L})$ steps. In [7], Zenner et al. proposed an attack that reconstructs the initial state of the generator from a short keystream sequence, requiring $\mathcal{O}(2^{0.694L})$ steps. On the other hand, Mihaljevic presented a faster attack that needs a longer part of keystream sequence in [6].

As a simulation, we applied Zhang et al.'s attack and our attack to the self-shrinking generator with the 240-bit internal state. Zhang et al.'s attack