Galois LFSR, Embedded Devices and Side Channel Weaknesses

Antoine Joux[1,2] and Pascal Delaunay[2,3]

[1] DGA
[2] Université de Versailles St-Quentin-en-Yvelines
PRISM
45, avenue des Etats-Unis
78035 Versailles Cedex, France
Antoine.Joux@m4x.org
[3] Thales
Pascal.DELAUNAY@fr.thalesgroup.com

Abstract. A new side channel attack against a simple LFSR is presented. The proposed attack targets a single Galois LFSR running on an embedded device where the only accessible information is the side channel leakage. Even if it is made only of simple XOR gates, such an object is vulnerable to side channel cryptanalysis depending on its implementation. Our attack combines simple side channel analysis and statistical analysis to guess output bits and fast correlation attack to recover the initial state. In practice, even if a LFSR is never used alone, this attack shows that simple XOR gates can reveal significant information in some circumstances.

1 Introduction

Since the introduction of Power Analysis Attacks by Kocher et al., Side Channel Analysis and Side Channel Resistance of cryptographic algorithms performed on embedded devices are being deeply studied. These attacks allow full recovery of secret data with relatively low complexity and small investment compared to mathematical cryptanalysis. Thus, the security of cryptographic algorithms on embedded devices is usually not only studied in a mathematical way but also in a side channel based approach.

While these attacks focus on key-dependent operations, values handled by the device and non-linear functions, elementary logic gates have rarely been studied in the literature. Moreover, stream ciphers, which are mainly composed of such gates, are not prime targets for side channel attacks. Still, there are a few publications on this topic such as [7] and [14]. We show in this paper that in the context of stream ciphers based on *Linear Feedback Shift Register* (LFSR) the leakage of XOR gates can be exploited in a Simple Side Channel Attack.

From the mathematical point of view, the security of LFSR based stream cipher as been deeply studied. In particular, correlation attacks are often considered. This class of attack studies how to recover the internal state of the

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 436–451, 2006.

underlying LFSR by viewing the output of the stream cipher as a noisy version of the LFSR output (modeled by a binary symmetric channel). It is especially useful when a good linear approximation of the output function can be found. Ordinary correlation attacks can only be applied to small LFSR where the internal state can by exhaustively searched. Thus they are often used in a divide and conquer manner against stream ciphers which rely on several small LFSRs. With larger LFSRs, it is possible to use fast correlation attacks which overcome this length limitation at the cost of using longer output sequences. These *Fast Correlation Attacks*, were introduced by Meier and Staffelbach [9], and have two different phases. The first and most time consuming consists in finding as many *parity check equations* as possible (low-weight linear relations between the output bits and the initial state). Many papers (e.g. see [10], [3], [4]) describe efficient methods to compute such equations. The second phase decodes the sequence observed to reconstruct the initial state of the LFSR.

LFSRs are often implemented as *divisor registers* (also known as Galois LFSRs) (Fig. 2) because they offer minimal latency and higher speed for the same output sequence. We show in the following that such an implementation is vulnerable to *Simple Side Channel Attacks*. From now on, we consider a n-bit length divisor register running on an embedded device where the only available information is the side channel leakage. This roughly models a strong mathematical LFSR based stream cipher, where the output function is cryptographically strong. In that case, the stream output does not offer any usable information to an attacker wishing to recover the secret key or equivalently the LFSR state. In this model, we exhibit a significant bias between the side channel leakage of the Galois LFSR and the value of the bit which is shifted out of the LFSR.

If the bias is large enough to correctly predict n consecutive output bits then simple linear algebra allows direct recovery of the initial state. However, the side channel analysis is often noisy so this extremely favorable case is unlikely to happen.

As a consequence, we mix the basic side channel approach with cryptanalytic tools in order to go further. More precisely, the side channel analysis produces a biased prediction of the Galois LFSR output bits. In order to make a simplified analysis, we assume that the prediction of different bits is independent and thus behave as in the Binary Symmetric Channel model (BSC). Since correlation and fast correlation attacks are already described in this model, it is of course natural to use them as a tool to amplify the side channel predictions and recover the LFSR initial state. In other words, the basic idea in this paper is to replace the correlation between LFSR output and stream cipher output usually used in correlation attacks by a side channel correlation. Note that in some cases, it could also be possible to combine both the side channel information and the stream cipher output in order to get an even better bias. We do not consider this variant in depth.

The present paper is organized as follows : in section 2 we recall the basics on LFSRs and divisor registers. Section 3 is devoted to Side Channel Attacks. We analyze the leakage induced by the XOR gates of our Galois LFSR with respect to two often used models : the *Hamming weight model* and the *Hamming distance*