Vectorial Approach to Fast Correlation Attacks∗

Jovan Dj. Golic
Access Network and Terminals System Design, Telecom Italia Lab, Via Guglielmo Reiss Romoli 274, 10148 Turin, Italy.

Philip Hawkes
Qualcomm Australia, 230 Victoria Rd, Gladesville, NSW, Australia

Communicated by: H. Imai
Received August 19, 2002; Revised February 28, 2003; Accepted May 19, 2003

Abstract.
A new, vectorial approach to fast correlation attacks on binary memoryless combiners is proposed. Instead of individual input sequences or their linear combinations, the new attack is targeting subsets of input sequences as a whole thus exploiting the full correlation between the chosen subset and the output sequence. In particular, the set of all the input sequences can be chosen as the target. The attack is based on a novel iterative probabilistic algorithm which is also applicable to general memoryless combiners over finite fields or finite rings. To illustrate the effectiveness of the introduced approach, experimental results obtained for random balanced combining functions are presented.

Keywords: vectorial correlation attack, linear cryptanalysis, iterative probabilistic decoding, finite fields, nonlinear filter generator

1. Introduction

Fast correlation attacks against binary linear feedback shift registers (LFSR's) and more general combiners for stream cipher applications are based on an earlier work on divide-and-conquer correlation attacks [17]. The attacks exploit the bitwise correlation between the keystream sequence and linear combinations of the LFSR sequences. As such, the attacks require the assumption of linear feedback shift registers (LFSR's) with feedback polynomials which are relatively small compared to the memoryless combiners. In this paper, we present a new, vectorial approach to fast correlation attacks which is applicable to memoryless combiners with memory.

∗ Most of this work was done while he was with Rome CryptoDesign Center, Gemplus, Italy.
The minimum distance decoding [17] for a time-invariant binary symmetric channel is not feasible.

The decoding techniques used in fast correlation attacks are based on the linear relations satisfied by the codeword bits which are called the parity checks. The parity checks correspond to polynomial multiples of the combined LFSR feedback polynomial. For the attacks to be effective, the parity checks should have a relatively low weight, i.e., should involve a small number of codeword bits. The techniques essentially reduce to (iterative) error-correction decoding algorithms for binary symmetric channels. They may be feasible for large $k$ and $N-k$. For example, an iterative hard-decision decoding technique [18] is based on the majority decision rule and in fact originates from [5], where a similar technique is based on a more sophisticated iteration principle, later called the belief propagation principle. An iterative soft-decision decoding technique first proposed in [12] and later improved in [13] essentially originates from [3] and [5], and is based on the posterior probability symbol-by-symbol decoding algorithm known as the Hartmann–Rudolph algorithm [9].

For a given set of parity checks used, the techniques based on soft-decision decoding are more effective than techniques based on hard-decision decoding, whereas iterative decoding techniques are more powerful than one-step decoding techniques. More precisely, they can deal with smaller correlation coefficients, at the expense of increased complexity. The required output sequence length and the complexity of such attacks mainly depend on the absolute value(s) of the exploited correlation coefficient(s) and on the degrees and numbers of low-weight polynomial multiples of the involved LFSR feedback polynomials.

A number of more recent contributions in the area of binary fast correlation attacks including [1, 2, 10, 14–16] investigate various complexity-performance tradeoffs achievable by using specific parity checks such as parity checks with memory or parity checks involving a fixed subset of codeword bits. For example, one approach is to simplify the decoding algorithms and use more parity checks instead. Typically, these techniques need a high precomputation complexity to generate the parity checks and require a long keystream sequence, but are applicable to arbitrary LFSR feedback polynomials.

One motivation for this paper is to generalize the binary fast correlation attacks to $q$-ary fast correlation attacks that can be applied to $q$-ary memoryless combinators, in which the LFSR sequences are defined over a finite field $\mathbb{F}_q$ or over a finite ring $\mathbb{Z}_q$. Such attacks are important for analyzing the keystream generators suitable for software applications, which typically utilize linear recurrences involving a small number of terms over $\mathbb{F}_q$ or $\mathbb{Z}_q$, where $q = 2^m$. They may also be interesting for finding low-order approximations to $q$-ary cryptographic functions depending on a large number of input variables (for binary cryptographic functions, see [6]).

However, the main objective of this paper is in fact to show that $q^m$-ary fast correlation attacks can be applied to $q^m$-ary memoryless combinators, thus simultaneously utilizing the correlations to different linear functions of $m$ inputs in a vectorial manner. In particular, for $q = 2$, the introduced vectorial correlation attacks...