Improved Message Passing Techniques in Fast Correlation Attacks on Stream Ciphers

Martin Ågren

Dept. of Electrical and Information Technology, Lund University,
P.O. Box 118, 221 00 Lund, Sweden
martin.agren@eit.lth.se

Stream ciphers constitute an important class of cryptographic primitives, suitable for performance-critical encryption and decryption. The fast correlation attack, originally introduced by Meier & Staffelbach, is a general cryptanalytic attack directed at stream ciphers constructed using linear feedback shift registers (LFSRs). The attack exploits low-weight multiples of the LFSR feedback polynomial. Fast correlation attacks are heavily related to the decoding of low-density parity-check (LDPC) codes as developed by Gallager. One standard approach to decoding LDPC codes is the message passing algorithm.

In coding, the code designer tries to choose a code with specific properties. In fast correlation attacks, however, the code that arises from the LFSR in the stream cipher cannot be changed by the cryptanalyst. Instead, they must try their best to decode it. While the code designer will generally avoid so-called non-orthogonal equations, the cryptanalyst should instead try to deal with them as efficiently as possible.

We show how to improve the message passing algorithm by exploiting the fact that the sum of an arbitrary number of initial state variables, called a fixed point, can be written as the sum of only a few other variables. Our algorithm manages to use the non-orthogonal multiples better than the standard message passing algorithm. This results in better use of information in the message passing algorithm. Simulations using multiples of weight 4 show that this added information results in better success probabilities for the attack.

Our technique may also find applications to LDPC codes with girth 4, although such codes are normally avoided.