

BDD-Attacks on Stream Ciphers

Dirk Stegemann

University of Mannheim, Germany

Abstract. Stream ciphers are primarily used for online-encryption of arbitrarily long data, for example when transmitting speech data between a Bluetooth headset and a mobile phone. Many practically used and intensively discussed stream ciphers consist of a small number of linear feedback shift registers (LFSRs) that transform a secret key $x \in \{0, 1\}^n$ into an output keystream of arbitrary length. In 2002, Krause showed how to use Binary Decision Diagrams (BDDs) to mount a generic attack on this type of ciphers that recovers the secret key from the shortest information-theoretically possible amount of output keystream. In the case of the Bluetooth cipher E_0 , this attack is the best currently known short-keystream attack. Unlike correlation attacks and algebraic attacks, the BDD-attack is also applicable to irregularly clocked stream ciphers like the GSM cipher A5/1. In this talk, we describe the BDD-attack and its application to A5/1 and E_0 in theory and practice, show how to reduce its memory consumption, and sketch some recent developments.