

Reducing the Memory Requirements of BDD-Attacks on LFSR-based Stream Ciphers

Matthias Krause and Dirk Stegemann

Theoretical Computer Science
University of Mannheim, Germany
{krause, stegemann}@th.informatik.uni-mannheim.de

The main application of stream ciphers is online-encryption of arbitrarily long data, for example when transmitting speech data between a Bluetooth-headset and a mobile GSM-phone or between the phone and a GSM base station. Examples for practically used and intensively discussed stream ciphers are the E_0 generator used in Bluetooth [1], the GSM cipher A5/1 [2], and the self-shrinking generator [4]. These ciphers consist of a small number of linear feedback shift registers (LFSRs) and a non-linear compression function $C : \{0, 1\}^* \rightarrow \{0, 1\}^*$. Based on a secret key $k \in \{0, 1\}^n$, the LFSRs produce an internal bitstream $z \in \{0, 1\}^*$ which is then transformed into an output keystream $y \in \{0, 1\}^*$ via $y = C(z)$. For a given plaintext stream p , the ciphertext stream c is computed by bitwise XORing the plaintext and the keystream, *i.e.*, $c_i = p_i \oplus y_i$ for all i . Any receiver who knows the secret key k can produce the keystream y himself and compute the plaintext bits as $p_i = c_i \oplus y_i$.

In 2002, Krause proposed a generic, Binary Decision Diagram (BDD) based attack [3] on this type of ciphers that reconstructs the internal bitstream z and thereby the secret key k from a short prefix of a given output keystream y . Currently, the BDD-attack is the best known short-keystream attack against E_0 and one of the best generic attacks against A5/1.

However, BDD-attacks require a large amount of memory. We approach this problem by presenting various efficiently parallelizable divide-and-conquer strategies (DCS) for E_0 and A5/1 that substantially reduce the memory requirements and allow us to tackle much larger keylengths with fixed computational resources. In the case of E_0 , our DCS lowers the attack's memory requirements by a factor of 2^{25} and slightly improves its runtime.

In [3], the application of the basic BDD-based attack to E_0 , A5/1 and the self-shrinking generator were theoretically described, but with rather pessimistic assumptions on the time and memory requirements. We present comprehensive experimental results for the BDD-attack on reduced versions of these ciphers, showing that the performance in practice does not substantially deviate from the theoretical figures.

References

- [1] The Bluetooth SIG. *Specification of the Bluetooth System*, February 2001.
- [2] M. Briceno, I. Goldberg, and D. Wagner. *A pedagogical implementation of A5/1*, May 1999. <http://jya.com/a51-pi.htm>.
- [3] M. Krause. BDD-based cryptanalysis of keystream generators. In *Proceedings of EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 222–237. Springer, 2002.
- [4] W. Meier and O. Staffelbach. The self-shrinking generator. In *Proceedings of EUROCRYPT 1994*, volume 950 of *LNCS*, pages 205–214. Springer, 1994.