Cryptanalysis of the full Spritz stream cipher

Spritz is a stream cipher proposed by Rivest and Schuldt at the rump session of CRYPTO 2014. It is intended to be a replacement of the popular RC4 stream cipher. In this paper we propose distinguishing attacks on the full Spritz, based on a short-term bias in the first two bytes of a keystream and a long-term bias in the first two bytes of every cycle of N keystream bytes, where N is the size of the internal permutation. Our attacks are able to distinguish a keystream of the full Spritz from a random sequence with samples of first two bytes produced by 244.8 multiple key-IV pairs or 260.8 keystream bytes produced by a single key-IV pair. These biases are also useful in the event of plaintext recovery in a broadcast attack. In the second part of the paper, we look at a state recovery attack on Spritz, in a special situation when the cipher enters a class of weak states. We determine the probability of encountering such a state, and demonstrate a state recovery algorithm that betters the 21400 step algorithm of Ankele et al. at Latincrypt 2015.