Cryptanalysis of the Fast Knapsack Generator

Florette Martinez

A pseudo-random number generator (PRNG) is an efficient deterministic algorithm that stretches a small random seed into a longer pseudo-random sequence of numbers. PRNGs are widely used in cryptographic protocols, especially for key generation. What we expect from these generators is unpredictability and computational indistinguishability of their outputs from a "true" random sequence as a security breach in a PRNG tends to spread to the whole cryptographic protocol where it is used.

The fast knapsack generator was introduced in 2009 by Von Zur Gathen and Shparlinski. It generates pseudo-random numbers very efficiently with strong mathematical guarantees on their statistical properties but its resistance to cryptanalysis was left open since 2009. In this presentation, we will present a practical seed-recovery attack on this PRNG when less than a quarter of the bits are discarded. This attack is based on the similarities this generator bears with an other family of PRNG: the Linear Congruential Generators (LCGs). We will use classical lattice-based tools for cryptography such as LLL or Coppersmith methods to attack the LCG and then lift our results to recover the seed of an instance of the fast knapsack generator.