The Dragon Is Alive and Well

Ed Dawson, Matt Henricksen, Willam Millan, and Leonie Simpson

Information Security Institute,
Queensland University of Technology,
GPO Box 2434, Brisbane,
Queensland, 4001, Australia.
{e.dawson, m.henricksen, b.millan, lr.simpson}@qut.edu.au

Dragon [1] is a word-based stream cipher operating on words of 32 bits. It is constructed using a non-linear feedback shift register modified by a non-linear filter function. Dragon, as submitted to ECRYPT, has two forms: Dragon-128, which specifies use with a 128-bit key and a 128-bit IV; and Dragon-256, which specifies use with a 256-bit key and a 256-bit IV.

Englund and Maximov [2] describe a distinguishing attack attack against Dragon-256, under the assumption that the cryptanalyst can obtain an enormous amount of keystream from a single key-IV pair, in violation of the designers' restriction on the maximum length of keystream to be produced before rekeying.

Both variants of the distinguishing attack require 2^{155} words of keystream. The first has an operational complexity of 2^{187} and uses 2^{32} words of memory. The second variant trades off memory for time with the resultant complexities of 2^{155} and 2^{96} for time and memory respectively. For both variants, the operational complexity is below the 2^{255} effort suggested by the design strength of the Dragon-256 cipher, but much greater than exhaustive search for the Dragon-128 cipher. Thus the Dragon-128 cipher is immune to this distinguishing attack. Even against Dragon-256, the complexity of the distinguishing attack is extremely large, making it infeasible in any practical sense. Note also that the keystream requirement for the distinguishing attack is in violation of the Dragon designers' recommendation. As stated in [1]:

> To protect against unknown future attacks, and against attacks that require large amounts of keystream, [Dragon] should be rekeyed at least once for every 2^{64} bits of keystream generated.

The distinguishing attack described by Englund and Maximov is possible only if the designers' restriction on keystream length is relaxed to allow the generation of enormous amounts of keystream under a single key-IV pair. The amount of keystream required is 2^{97} times the 2^{64} bit maximum recommended.

The designers concur that the distinguisher does occur with the probabilities stated by Englund and Maximov. Dragon uses a repeated 32×32 mapping constructed from two 8×32 s-boxes in such a way that only 16% of the outputs are accessible. This leads to the keystream bias theoretically detected and empirically measured by Englund et al. at $2^{-74.515}$. While of some theoretical interest, it seems unlikely that this distinguisher can be turned into a key recovery attack with a complexity less than that of a brute force attack.

Dragon-128 is immune to the distinguishing attack proposed by Englund and Maximov, as is Dragon-256 as specified for ECRYPT. That is, if the designers' restriction on the maximum keystream length permitted before rekeying is respected. Thus, although of some theoretical interest, we don't believe the keystream bias noted by Englund and Maximov represents a significant weakness in the Dragon cipher, nor can that bias be exploited in a key recovery attack. We do not believe that the distinguishing attack endangers the security of the Dragon cipher and consequently we are happy for Dragon to remain in ECRYPT.

References

1. Kevin Chen, Matt Henricksen, Leonie Simpson, William Millian, and Ed Dawson. Dragon: A fast word based cipher. In Choonsik Park and Seongtaek Chee, editors, *Information Security and Cryptology - ICISC '04 - Seventh International Conference*, volume 3506 of *Lecture Notes in Computer Science*, pages 33–50, 2004.
2. Hakan Englund and Alexander Maximov. Attack the Dragon, 2005. Available at http://www.ecrypt.eu.org/stream/papersdir/062.pdf.