Pypy: Another Version of Py

Eli Biham, Jennifer Seberry

Department of Computer Science
Technion, Haifa 32000, Israel

March 16, 2006

Py

1. Stream cipher
2. Submitted to eStream
3. Very fast: 2.85 cycles/byte on Pentium (RC4 takes 7).
4. It uses rotating arrays, and ideas similar to RC4
5. Outputs two 32-bit words at a time
6. Has another version Py6

Pypy (Pronounced Roopy or Rupee)

1. The original version of Py
2. Provides extra security over Py, for those applications for which distinguishing attacks that require more than 2^{64} bytes of streams (thus from many streams with many keys) is not secure enough
3. Runs at speeds of about 4–4.5 cycles/byte
4. Outputs only the first word of every two words of Py
5. Identical to Py in any other sense
6. We will ask eStream to consider Pypy, in addition to the current candidates Py and Py6

Pseudocode of Pypy

1. Use Py
2. Setup the key and IV as in Py
3. Run Py with twice the size of the required output
4. Select every second word of the generated key stream (starting with the first word)

A Pypy in the Hand is Worth more than

in the Bush

The End