UNIVERSITÉ DU LUXEMBOURG

Dear Professor Bart Preneel

By this I would like to submit a tweak of a stream cipher design named "LEX" to the ECRYPT call for stream cipher primitive. The tweak applies to all the three proposed key sizes 128/192/256-bit of the original LEX proposal and takes care of the sliding property which is undesirable for key sizes 192/256.

Here are the cover sheet details:

1. **Name of the algorithm**: LEX-128, LEX-192, LEX-256.
2. **Type of algorithm**: Synchronous 128/192/256-bit key stream cipher. Profile 1, Profile 2.
3. **Claimed security level**: 2^128, 2^160, 2^192 (taking into account multiple target tradeoff attacks. Not taking into account throughput complexity measure used in parallel hardware attacks.)
4. **Usage:** Change the key every 2^32 IV setups, and change the IV every 500 iterations.
5. **Principal submitter**: Alex Biryukov,
   Phone: +352 46 66 44 6793
   FAX: +352 46 66 44 6793
   FDEF, University of Luxembourg
   162 A, Avenue de la Faiencerie
   L-1511 Luxembourg, LUXEMBOURG.
6. **E-mail**: alex.biryukov AT uni.lu
7. **Homepage**: http://www.esat.kuleuven.ac.be/~abiryuko/
8. **Names of auxiliary submitters**: None
9. **Name of algorithm inventor**: Alex Biryukov.
10. **Name of owner**: Alex Biryukov, the algorithm is put in public domain.

Sincerely yours,

Alex Biryukov