HAZAR STREAM CIPHER

Intoduction

Hazar is a stream cipher that has a new outlook for key schedule. It generates unique key for every sequence with pseudo random generator style key schedule. Basicly, key schedule algorithm generates one-way, highly random key and the key xored with data.

Hazar algorithm uses very large key size (for hazar8: 2048 bit, for hazar64: 524288 bit). General idea of this cipher is to be resistant to quantum computing era with large keys and good PRNG properties. As seen absurdly gigantic key size; Hazar64 is same algorithm only different key size created for preventing brute force attacks from predicted possible “super quantum cluster computers”.

Note #1: As the nature of stream ciphers, data and key is same size at operation.
Note #2: Algorithm is executed same for encryption and decryption. Current encryption mode does not feedbacks previous cipher block.

Key Schedule

Key schedule is actually simple but requires very recursive calculations at generation. User supplies key and length of key. With this initial information we need to fill 2 S-Boxes. At the proceeding steps, this two S-Boxes re-calculated and used only one time for each key block. Key length is also used at initial iteration sequence. Regardless of key length, algorithm also carries out fixed number of iterations for maximum security. (For hazar8: 256, for hazar64: 65536)

Key iterations uses 2 s-box for virtual idea of substitution of **data** and substitution of **order of data**. With these 2 variables, s-box values used and xored. Generated key also reused after mixing s-box for next sequence. Key always mixes s-boxes and s-boxes always generates new key. (Hopefully)

Encryption / Decryption

This process is very simple. Just data xored with currently generated key. Encryption and decryption is exactly same but must be started from beginning.

Test Results

We used 2 files. One filled with zeroes and one created with random values from Linux /dev/random device. We used 2 commands to test file randomness. (ent and diehard)

Note: Tests carried out in Linux system! Please use “man ent” and “man dieharder” for more information.

- Source File: zero.dat (2 GB)
- Used Password: Password (8 chars)

Executed Test (ent)
Results;

```
Entropy = 8.000000 bits per byte.
Optimum compression would reduce the size
of this 2147483912 byte file by 0 percent.
Chi square distribution for 2147483912 samples is 265.69, and randomly
would exceed this value 30.98 percent of the times.
Arithmetic mean value of data bytes is 127.4962 (127.5 = random).
Monte Carlo value for Pi is 3.141630255 (error 0.00 percent).
Serial correlation coefficient is -0.000003 (totally uncorrelated = 0.0).
```

HAZAR STREAM CIPHER

Executed Test (dieharder)
Results;

```
#==================================================================================#
#            dieharder version 3.31.1 Copyright 2003 Robert G. Brown               #
#==================================================================================#
   rng_name    |           filename             |rands/second|
 file_input_raw|                     zero.dat.enc|  6.52e+07  |
#==================================================================================#
        test_name   |ntup| tsamples |psamples|  p-value |Assessment
#==================================================================================#
   diehard_birthdays|   0|       100|     100|0.21541675|  PASSED
      diehard_operm5|   0|   1000000|     100|0.86882994|  PASSED
  diehard_rank_32x32|   0|     40000|     100|0.58710723|  PASSED
    diehard_rank_6x8|   0|    100000|     100|0.69666971|  PASSED
   diehard_bitstream|   0|   2097152|     100|0.68263537|  PASSED
        diehard_opso|   0|   2097152|     100|0.88398416|  PASSED
        diehard_oqso|   0|   2097152|     100|0.70528601|  PASSED
         diehard_dna|   0|   2097152|     100|0.69936765|  PASSED
diehard_count_1s_str|   0|    256000|     100|0.74670328|  PASSED
diehard_count_1s_byt|   0|    256000|     100|0.95032125|  PASSED
 diehard_parking_lot|   0|     12000|     100|0.98287267|  PASSED
    diehard_2dsphere|   2|      8000|     100|0.83531579|  PASSED
    diehard_3dsphere|   3|      4000|     100|0.99292257|  PASSED
     diehard_squeeze|   0|    100000|     100|0.29187892|  PASSED
        diehard_sums|   0|       100|     100|0.18021405|  PASSED
        diehard_runs|   0|    100000|     100|0.73775208|  PASSED
        diehard_runs|   0|    100000|     100|0.29411874|  PASSED
       diehard_craps|   0|    200000|     100|0.94030939|  PASSED
       diehard_craps|   0|    200000|     100|0.20117247|  PASSED
 marsaglia_tsang_gcd|   0|  10000000|     100|0.51281917|  PASSED
 marsaglia_tsang_gcd|   0|  10000000|     100|0.26612770|  PASSED
         sts_monobit|   1|    100000|     100|0.40028393|  PASSED
            sts_runs|   2|    100000|     100|0.63871344|  PASSED
          sts_serial|   1|    100000|     100|0.51048115|  PASSED
          sts_serial|   2|    100000|     100|0.69888537|  PASSED
          sts_serial|   3|    100000|     100|0.77294116|  PASSED
          sts_serial|   3|    100000|     100|0.40337934|  PASSED
          sts_serial|   4|    100000|     100|0.99103251|  PASSED
          sts_serial|   4|    100000|     100|0.90710689|  PASSED
          sts_serial|   5|    100000|     100|0.90944458|  PASSED
          sts_serial|   5|    100000|     100|0.95639033|  PASSED
          sts_serial|   6|    100000|     100|0.89616002|  PASSED
          sts_serial|   6|    100000|     100|0.62929322|  PASSED
          sts_serial|   7|    100000|     100|0.56650564|  PASSED
          sts_serial|   7|    100000|     100|0.42526054|  PASSED
          sts_serial|   8|    100000|     100|0.77663243|  PASSED
          sts_serial|   8|    100000|     100|0.80239762|  PASSED
          sts_serial|   9|    100000|     100|0.99037360|  PASSED
          sts_serial|   9|    100000|     100|0.64760097|  PASSED
          sts_serial|  10|    100000|     100|0.96302426|  PASSED
          sts_serial|  10|    100000|     100|0.99930635|   WEAK
          sts_serial|  11|    100000|     100|0.65466835|  PASSED
          sts_serial|  11|    100000|     100|0.84625711|  PASSED
          sts_serial|  12|    100000|     100|0.43584698|  PASSED
```

sts_serial	12	100000	100	0.08579792	PASSED
sts_serial	13	100000	100	0.58952631	PASSED
sts_serial	13	100000	100	0.88326934	PASSED
sts_serial	14	100000	100	0.97998987	PASSED
sts_serial	14	100000	100	0.67193696	PASSED
sts_serial	15	100000	100	0.77078392	PASSED
sts_serial	15	100000	100	0.56776673	PASSED
sts_serial	16	100000	100	0.53707939	PASSED
sts_serial	16	100000	100	0.03829097	PASSED
rgb_bitdist	1	100000	100	0.74116463	PASSED
rgb_bitdist	2	100000	100	0.23411375	PASSED
rgb_bitdist	3	100000	100	0.82437572	PASSED
rgb_bitdist	4	100000	100	0.03748833	PASSED
rgb_bitdist	5	100000	100	0.94355914	PASSED
rgb_bitdist	6	100000	100	0.89785281	PASSED
rgb_bitdist	7	100000	100	0.71876087	PASSED
rgb_bitdist	8	100000	100	0.82233635	PASSED
rgb_bitdist	9	100000	100	0.02005956	PASSED
rgb_bitdist	10	100000	100	0.38500016	PASSED
rgb_bitdist	11	100000	100	0.60562775	PASSED
rgb_bitdist	12	100000	100	0.99984464	WEAK
rgb_minimum_distance	2	10000	1000	0.61740608	PASSED
rgb_minimum_distance	3	10000	1000	0.17614912	PASSED
rgb_minimum_distance	4	10000	1000	0.17404760	PASSED
rgb_minimum_distance	5	10000	1000	0.11953808	PASSED
rgb_permutations	2	100000	100	0.93220621	PASSED
rgb_permutations	3	100000	100	0.11388481	PASSED
rgb_permutations	4	100000	100	0.27740252	PASSED
rgb_permutations	5	100000	100	0.83206222	PASSED
rgb_lagged_sum	0	1000000	100	0.83211552	PASSED
rgb_lagged_sum	1	1000000	100	0.86897592	PASSED
rgb_lagged_sum	2	1000000	100	0.48478539	PASSED
rgb_lagged_sum	3	1000000	100	0.28137705	PASSED
rgb_lagged_sum	4	1000000	100	0.92716097	PASSED
rgb_lagged_sum	5	1000000	100	0.00254178	WEAK
rgb_lagged_sum	6	1000000	100	0.99596345	WEAK
rgb_lagged_sum	7	1000000	100	0.99565742	WEAK
rgb_lagged_sum	8	1000000	100	0.92024662	PASSED
rgb_lagged_sum	9	1000000	100	0.01066947	PASSED
rgb_lagged_sum	10	1000000	100	0.11330606	PASSED
rgb_lagged_sum	11	1000000	100	0.21126254	PASSED
rgb_lagged_sum	12	1000000	100	0.11261122	PASSED
rgb_lagged_sum	13	1000000	100	0.76622215	PASSED
rgb_lagged_sum	14	1000000	100	0.20123902	PASSED
rgb_lagged_sum	15	1000000	100	0.04316976	PASSED
rgb_lagged_sum	16	1000000	100	0.48038274	PASSED
rgb_lagged_sum	17	1000000	100	0.02559523	PASSED
rgb_lagged_sum	18	1000000	100	0.03438639	PASSED
rgb_lagged_sum	19	1000000	100	0.21522617	PASSED
rgb_lagged_sum	20	1000000	100	0.89816382	PASSED
rgb_lagged_sum	21	1000000	100	0.02649329	PASSED
rgb_lagged_sum	22	1000000	100	0.10241938	PASSED
rgb_lagged_sum	23	1000000	100	0.02711551	PASSED
rgb_lagged_sum	24	1000000	100	0.00248941	WEAK
rgb_lagged_sum	25	1000000	100	0.02861454	PASSED
rgb_lagged_sum	26	1000000	100	0.08893707	PASSED
rgb_lagged_sum	27	1000000	100	0.37837193	PASSED

HAZAR STREAM CIPHER

```
      rgb_lagged_sum|  28|   1000000|     100|0.33594007|  PASSED
      rgb_lagged_sum|  29|   1000000|     100|0.34275588|  PASSED
      rgb_lagged_sum|  30|   1000000|     100|0.73332808|  PASSED
      rgb_lagged_sum|  31|   1000000|     100|0.91705085|  PASSED
      rgb_lagged_sum|  32|   1000000|     100|0.28473712|  PASSED
     rgb_kstest_test|   0|     10000|    1000|0.88603952|  PASSED
     dab_bytedistrib|   0|  51200000|       1|0.69517423|  PASSED
             dab_dct| 256|     50000|       1|0.56628701|  PASSED
Preparing to run test 207.  ntuple = 0
        dab_filltree|  32|  15000000|       1|0.86973215|  PASSED
        dab_filltree|  32|  15000000|       1|0.33785767|  PASSED
Preparing to run test 208.  ntuple = 0
       dab_filltree2|   0|   5000000|       1|0.70106163|  PASSED
       dab_filltree2|   1|   5000000|       1|0.11802286|  PASSED
Preparing to run test 209.  ntuple = 0
        dab_monobit2|  12|  65000000|       1|0.69942658|  PASSED
```

- Source File: rand.dat (2 GB)
- Used Password: Password (8 chars)

Executed Test (ent)
Results;

```
Entropy = 8.000000 bits per byte.
Optimum compression would reduce the size
of this 2147483912 byte file by 0 percent.
Chi square distribution for 2147483912 samples is 246.91, and randomly
would exceed this value 63.02 percent of the times.
Arithmetic mean value of data bytes is 127.5031 (127.5 = random).
Monte Carlo value for Pi is 3.141451542 (error 0.00 percent).
Serial correlation coefficient is 0.000017 (totally uncorrelated = 0.0).
```

Executed Test (dieharder)
Results;

```
#=============================================================================#
#            dieharder version 3.31.1 Copyright 2003 Robert G. Brown          #
#=============================================================================#
   rng_name    |           filename             |rands/second|
 file_input_raw|                    rand.dat.enc|  7.33e+07  |
#=============================================================================#
        test_name   |ntup| tsamples |psamples|  p-value |Assessment
#=============================================================================#
   diehard_birthdays|   0|       100|     100|0.80860060|  PASSED
      diehard_operm5|   0|   1000000|     100|0.02837892|  PASSED
  diehard_rank_32x32|   0|     40000|     100|0.64790071|  PASSED
    diehard_rank_6x8|   0|    100000|     100|0.36035454|  PASSED
   diehard_bitstream|   0|   2097152|     100|0.95008050|  PASSED
        diehard_opso|   0|   2097152|     100|0.91878419|  PASSED
        diehard_oqso|   0|   2097152|     100|0.63613678|  PASSED
         diehard_dna|   0|   2097152|     100|0.66467625|  PASSED
diehard_count_1s_str|   0|    256000|     100|0.94139195|  PASSED
diehard_count_1s_byt|   0|    256000|     100|0.72627114|  PASSED
 diehard_parking_lot|   0|     12000|     100|0.79600924|  PASSED
    diehard_2dsphere|   2|      8000|     100|0.96506355|  PASSED
    diehard_3dsphere|   3|      4000|     100|0.39523819|  PASSED
```

HAZAR STREAM CIPHER

```
     diehard_squeeze|   0|    100000|     100|0.75692112|  PASSED
        diehard_sums|   0|       100|     100|0.18921863|  PASSED
        diehard_runs|   0|    100000|     100|0.99651783|   WEAK
        diehard_runs|   0|    100000|     100|0.42112658|  PASSED
       diehard_craps|   0|    200000|     100|0.93650826|  PASSED
       diehard_craps|   0|    200000|     100|0.47175394|  PASSED
 marsaglia_tsang_gcd|   0|  10000000|     100|0.59997069|  PASSED
 marsaglia_tsang_gcd|   0|  10000000|     100|0.55724952|  PASSED
         sts_monobit|   1|    100000|     100|0.64904677|  PASSED
            sts_runs|   2|    100000|     100|0.92751028|  PASSED
          sts_serial|   1|    100000|     100|0.72464548|  PASSED
          sts_serial|   2|    100000|     100|0.77669776|  PASSED
          sts_serial|   3|    100000|     100|0.96990810|  PASSED
          sts_serial|   3|    100000|     100|0.74124068|  PASSED
          sts_serial|   4|    100000|     100|0.82071523|  PASSED
          sts_serial|   4|    100000|     100|0.86183647|  PASSED
          sts_serial|   5|    100000|     100|0.51207146|  PASSED
          sts_serial|   5|    100000|     100|0.17173213|  PASSED
          sts_serial|   6|    100000|     100|0.56309351|  PASSED
          sts_serial|   6|    100000|     100|0.21370797|  PASSED
          sts_serial|   7|    100000|     100|0.49670370|  PASSED
          sts_serial|   7|    100000|     100|0.78518105|  PASSED
          sts_serial|   8|    100000|     100|0.70161794|  PASSED
          sts_serial|   8|    100000|     100|0.85211932|  PASSED
          sts_serial|   9|    100000|     100|0.69098361|  PASSED
          sts_serial|   9|    100000|     100|0.44212632|  PASSED
          sts_serial|  10|    100000|     100|0.20640322|  PASSED
          sts_serial|  10|    100000|     100|0.10556121|  PASSED
          sts_serial|  11|    100000|     100|0.82623966|  PASSED
          sts_serial|  11|    100000|     100|0.67241802|  PASSED
          sts_serial|  12|    100000|     100|0.83983609|  PASSED
          sts_serial|  12|    100000|     100|0.47431778|  PASSED
          sts_serial|  13|    100000|     100|0.67294660|  PASSED
          sts_serial|  13|    100000|     100|0.09422185|  PASSED
          sts_serial|  14|    100000|     100|0.51928199|  PASSED
          sts_serial|  14|    100000|     100|0.42332832|  PASSED
          sts_serial|  15|    100000|     100|0.90153788|  PASSED
          sts_serial|  15|    100000|     100|0.32416555|  PASSED
          sts_serial|  16|    100000|     100|0.74833377|  PASSED
          sts_serial|  16|    100000|     100|0.94543354|  PASSED
         rgb_bitdist|   1|    100000|     100|0.51813617|  PASSED
         rgb_bitdist|   2|    100000|     100|0.97674941|  PASSED
         rgb_bitdist|   3|    100000|     100|0.91595714|  PASSED
         rgb_bitdist|   4|    100000|     100|0.84992659|  PASSED
         rgb_bitdist|   5|    100000|     100|0.14055517|  PASSED
         rgb_bitdist|   6|    100000|     100|0.65989794|  PASSED
         rgb_bitdist|   7|    100000|     100|0.81916907|  PASSED
         rgb_bitdist|   8|    100000|     100|0.07783534|  PASSED
         rgb_bitdist|   9|    100000|     100|0.45013130|  PASSED
         rgb_bitdist|  10|    100000|     100|0.90102365|  PASSED
         rgb_bitdist|  11|    100000|     100|0.40050840|  PASSED
         rgb_bitdist|  12|    100000|     100|0.62083632|  PASSED
rgb_minimum_distance|   2|     10000|    1000|0.09439766|  PASSED
rgb_minimum_distance|   3|     10000|    1000|0.29344102|  PASSED
rgb_minimum_distance|   4|     10000|    1000|0.69992457|  PASSED
rgb_minimum_distance|   5|     10000|    1000|0.78370507|  PASSED
    rgb_permutations|   2|    100000|     100|0.56273791|  PASSED
```

```
    rgb_permutations|   3|    100000|     100|0.76453884|  PASSED
    rgb_permutations|   4|    100000|     100|0.62313191|  PASSED
    rgb_permutations|   5|    100000|     100|0.47228947|  PASSED
      rgb_lagged_sum|   0|   1000000|     100|0.14453451|  PASSED
      rgb_lagged_sum|   1|   1000000|     100|0.50826186|  PASSED
      rgb_lagged_sum|   2|   1000000|     100|0.89049665|  PASSED
      rgb_lagged_sum|   3|   1000000|     100|0.94666441|  PASSED
      rgb_lagged_sum|   4|   1000000|     100|0.96837860|  PASSED
      rgb_lagged_sum|   5|   1000000|     100|0.68298460|  PASSED
      rgb_lagged_sum|   6|   1000000|     100|0.84978325|  PASSED
      rgb_lagged_sum|   7|   1000000|     100|0.98445583|  PASSED
      rgb_lagged_sum|   8|   1000000|     100|0.57205965|  PASSED
      rgb_lagged_sum|   9|   1000000|     100|0.99408363|  PASSED
      rgb_lagged_sum|  10|   1000000|     100|0.51803069|  PASSED
      rgb_lagged_sum|  11|   1000000|     100|0.85504606|  PASSED
      rgb_lagged_sum|  12|   1000000|     100|0.80864466|  PASSED
      rgb_lagged_sum|  13|   1000000|     100|0.03046744|  PASSED
      rgb_lagged_sum|  14|   1000000|     100|0.00501734|  PASSED
      rgb_lagged_sum|  15|   1000000|     100|0.20800076|  PASSED
      rgb_lagged_sum|  16|   1000000|     100|0.11639579|  PASSED
      rgb_lagged_sum|  17|   1000000|     100|0.93112480|  PASSED
      rgb_lagged_sum|  18|   1000000|     100|0.02599000|  PASSED
      rgb_lagged_sum|  19|   1000000|     100|0.71928459|  PASSED
      rgb_lagged_sum|  20|   1000000|     100|0.78206442|  PASSED
      rgb_lagged_sum|  21|   1000000|     100|0.44858402|  PASSED
      rgb_lagged_sum|  22|   1000000|     100|0.45300897|  PASSED
      rgb_lagged_sum|  23|   1000000|     100|0.53343312|  PASSED
      rgb_lagged_sum|  24|   1000000|     100|0.46026884|  PASSED
      rgb_lagged_sum|  25|   1000000|     100|0.74542219|  PASSED
      rgb_lagged_sum|  26|   1000000|     100|0.96455645|  PASSED
      rgb_lagged_sum|  27|   1000000|     100|0.20505610|  PASSED
      rgb_lagged_sum|  28|   1000000|     100|0.56165783|  PASSED
      rgb_lagged_sum|  29|   1000000|     100|0.52979062|  PASSED
      rgb_lagged_sum|  30|   1000000|     100|0.60064826|  PASSED
      rgb_lagged_sum|  31|   1000000|     100|0.37765892|  PASSED
      rgb_lagged_sum|  32|   1000000|     100|0.21226521|  PASSED
     rgb_kstest_test|   0|     10000|    1000|0.63033721|  PASSED
     dab_bytedistrib|   0|  51200000|       1|0.90020688|  PASSED
            dab_dct| 256|     50000|       1|0.30038002|  PASSED
Preparing to run test 207.  ntuple = 0
        dab_filltree|  32|  15000000|       1|0.53812989|  PASSED
        dab_filltree|  32|  15000000|       1|0.42714359|  PASSED
Preparing to run test 208.  ntuple = 0
       dab_filltree2|   0|   5000000|       1|0.12308001|  PASSED
       dab_filltree2|   1|   5000000|       1|0.29691217|  PASSED
Preparing to run test 209.  ntuple = 0
        dab_monobit2|  12|  65000000|       1|0.84814754|  PASSED
```