1 PRG270: Temperaturtests von Zufalls-Rohdaten

2 AIS31 evaluation tests kurz bei +20°C

```
*************************************************************************
*                                                                       *
*                        AIS31 evaluation tests                         *
*                                                                       *
*************************************************************************


date, time:     06/13/2019,  17:36:02
tested file:    T+20.rnd
size of file:   10485760 bytes


-------------------------------------------------------------------------
Introduction
-------------------------------------------------------------------------

The purpose of the following tests is to evaluate the suitability
of a true (physical) random number generator for cryptographic
applications. In [1] an evaluation methodology for physical random
number generators has been proposed by the German Federal Security
Agency. In the mathematical-technical reference to [1], five tests
are defined for the P2-evaluation of a physical random number
generator (cf. [3] and [4]) which are implemented in the following
tests 1 - 5.


-------------------------------------------------------------------------
Results of test 1  (test (P2.i)(vii.a) of AIS 31, cf. [3] and [4])
-------------------------------------------------------------------------

In this test, the relative frequency r of bit 1 ocurring in the
first 100000 bits of the bit sequence is computed. Then the bit
sequence passes the test if |r - 0.5| < 0.025.

test scope:  first 100000 bits
number of ones:  49726
relative frequency:  0.497260
test value:  0.00274000  < 0.025

sequence passes test 1


-------------------------------------------------------------------------
Results of test 2  (test (P2.i)(vii.b) of AIS 31, cf. [3] and [4])
-------------------------------------------------------------------------

In this test, two disjoint sub-sequences TF(0) and TF(1) of bit pairs
are considered where TF(i) consists of the first 100000 bit pairs
of the form (i,x) ocurring in the bit sequence after the test scope
of test 1. Let v(i,j) denote the relative frequency of all bit pairs
of the form (i,j) in TF(i). Then the bit sequence passes the test
if |v(0,1) + v(1,0) - 1| < 0.02.

number of 2-bit words looked up: 202654
relative frequency v(0,1):  0.496070
relative frequency v(1,0):  0.504490
test value:  0.00056000 < 0.02

sequence passes test 2


-------------------------------------------------------------------------
Results of test 3  (test (P2.i)(vii.c) of AIS 31, cf. [3] and [4])
-------------------------------------------------------------------------

In this test, 4 disjoint sub-sequences TF(0,0),..., TF(1,1) of
3-tupels are considered where TF(i,j) consists of the first 100000
```

3-tupels of bits of the form (i,j,x) ocurring in the bit sequence
after the test scope of test 2. For every i,j in {0,1}, let S(i,j)
denote the sub-sequence of all bits k such that (i,j,k) is element
of TF(i,j). Then sample S(0,j) is compared with S(1,j) for every
j = 0,1. In this context, a comparison of two bit sequences g and h
of equal length is performed by a computation of the test value
t = (g_0 - h_0)^2 /(g_0 + h_0) + (g_1 - h_1)^2 /(g_1 + h_1) where
g_i resp. h_i is the number of bit i occurring in sequence g resp. h.
Let t_j be the test value for the comparison of S(0,j) with S(1,j)
Then the bit sequence passes the test if t_j < 15,13 for j = 0,1.

number of 3-bit words looked up: 406963
test value t_1:   0.030422 <= 15.13
test value t_2:   0.098004 <= 15.13

sequence passes test 3

Results of test 4 (test (P2.i)(vii.d) of AIS 31, cf. [3] and [4])

In this test, 8 disjoint sub-sequences TF(0,0,0),..., TF(1,1,1) of
4-tupels are considered where TF(i,j,k) consists of the first 100000
4-tupels of bits of the form (i,j,k,x) ocurring in the bit sequence
after the test scope of test 3. For every i,j in {0,1}, let S(i,j,k)
denote the sub-sequence of all bits b such that (i,j,k,b) is an
element of TF(i,j,k). Then sample S(0,j,k) is compared with S(1,j,k)
for every j,k of {0,1}. In this context, a comparison of two bit
sequences g and h of equal length is performed by a computation of the
test value t = (g_0 - h_0)^2 /(g_0 + h_0) + (g_1 - h_1)^2 /(g_1 + h_1)
where g_i resp. h_i is the number of bit i occurring in sequence g
resp. h. Let t_jk be the test value for the comparison of S(0,j,k)
with S(1,j,k). Then the bit sequence passes the test if t_jk < 15,13
for all j,k of {0,1}.

number of 4-bit words looked up: 818724
test value t_00:   0.137793 <= 15.13
test value t_01:   0.865326 <= 15.13
test value t_10:   0.044184 <= 15.13
test value t_11:   0.242010 <= 15.13

sequence passes test 4

Results of test 5 (test (P2.i)(vii.e) of AIS 31, cf. [3] and [4])

In this test, the Coron test with the parameters L = 8, Q = 2560,
and K = 256000 is performed (cf. [2]). For the first Q+K 8-bit-words
after the test scope of test 4, the test value f of the Coron test is
computed. The bit sequence passes the test if f > 7.976.

8-bit words looked up: 2560 + 256000 bytes
f-value: 8.00323282
8.00323282 > 7.976

sequence passes test 5

References
---

[1] AIS 31: Functionality Classes and Evaluation Methodology for
     Physical Random Number Generators. Version 1 (25.09.2001),
     (mandatory if a German IT security certificate is applied for;
     English translation).
     available at www.bsi.bund.de/zertifiz/zert/interpr/ais31e.pdf

[2] J.- S. Coron: On the Security of Random Sources. In: Public Key
     Cryptography - PKC 99. Lecture Notes in Computer Science,
     Vol. 1560, 29-42, Springer-Verlag, 2002.

[3] W. Killmann and W. Schindler: A Proposal for: Functionality
     Classes and Evaluation Methodology for True (Physical) Random
     Number Generators. Version 3.1 (25.09.2001), mathematical-
     technical reference of [1] (English Translation);

available at www.bsi.bund.de/zertifiz/zert/interpr/trngk31e.pdf

[4] W. Schindler and W. Killmann: Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications. In: Cryptographic Hardware and Empedded Systems - CHES 2002. Lecture Notes in Computer Science, Vol. 2523, 431-449, Springer-Verlag, 2002.

3 AIS31 evaluation tests lang bei +20°C

```
##########################################################################
#                                                                        #
#                          Results of RawTest                            #
#                                                                        #
##########################################################################


date, time:    06/13/2019,  17:36:19
tested file:   T+20.rnd
size of file:  10485760 bytes


**************************************************************************
*                                                                        *
*                    Results of the frequency test                       *
*                                                                        *
**************************************************************************


test scope:     first 10485760 bytes
relative frequency of bit 1:  0.49575278

block length L =  2:  chi^2 =     0.2475,  p-value = 0.96958745
block length L =  3:  chi^2 =     6.6295,  p-value = 0.46844829
block length L =  4:  chi^2 =    12.7708,  p-value = 0.61999760
block length L =  5:  chi^2 =    23.4550,  p-value = 0.83213728
block length L =  6:  chi^2 =    45.4447,  p-value = 0.95329789
block length L =  7:  chi^2 =    92.2617,  p-value = 0.99122236
block length L =  8:  chi^2 =   274.9371,  p-value = 0.18669114
block length L =  9:  chi^2 =   520.1302,  p-value = 0.38028245
block length L = 10:  chi^2 =  1035.2874,  p-value = 0.38771005


**************************************************************************
*                                                                        *
*                      Results of the serial test                        *
*                                                                        *
**************************************************************************


test scope:     first 10000000 bytes
relative frequency of bit 1:  0.49574462

block length L =  2:  chi^2 =     0.2426,  p-value = 0.88577211
block length L =  3:  chi^2 =     2.5971,  p-value = 0.62734535
block length L =  4:  chi^2 =     6.0652,  p-value = 0.63993243
block length L =  5:  chi^2 =    12.1081,  p-value = 0.73650628
block length L =  6:  chi^2 =    22.3520,  p-value = 0.89770633
block length L =  7:  chi^2 =    47.2865,  p-value = 0.94174029
block length L =  8:  chi^2 =   106.9499,  p-value = 0.91201843
block length L =  9:  chi^2 =   239.3331,  p-value = 0.76533514
block length L = 10:  chi^2 =   505.1350,  p-value = 0.57716175


**************************************************************************
*                                                                        *
*                  Results of the modular monobit test                   *
*                                                                        *
**************************************************************************
```

```
test scope:     first 10485760 bytes
relative frequency of bit 1:  0.49575278

modular monobit test for block length L = 3:
bit  0:  rf = 0.49585820, chi^2 =  1.24330253, p-value = 0.26483552
bit  1:  rf = 0.49568987, chi^2 =  0.44264521, p-value = 0.50584848
bit  2:  rf = 0.49571025, chi^2 =  0.20224997, p-value = 0.65291083

modular monobit test for block length L = 4:
bit  0:  rf = 0.49590201, chi^2 =  1.86844671, p-value = 0.17165309
bit  1:  rf = 0.49567728, chi^2 =  0.47814588, p-value = 0.48926336
bit  2:  rf = 0.49565525, chi^2 =  0.79791058, p-value = 0.37171881
bit  3:  rf = 0.49577656, chi^2 =  0.04744902, p-value = 0.82756316

modular monobit test for block length L = 5:
bit  0:  rf = 0.49573743, chi^2 =  0.01579751, p-value = 0.89997880
bit  1:  rf = 0.49568355, chi^2 =  0.32161410, p-value = 0.57063924
bit  2:  rf = 0.49589741, chi^2 =  1.40400230, p-value = 0.23605460
bit  3:  rf = 0.49577767, chi^2 =  0.04158076, p-value = 0.83842101
bit  4:  rf = 0.49566782, chi^2 =  0.48444552, p-value = 0.48641555

modular monobit test for block length L = 6:
bit  0:  rf = 0.49590877, chi^2 =  1.36101671, p-value = 0.24336135
bit  1:  rf = 0.49574634, chi^2 =  0.00231767, p-value = 0.96160294
bit  2:  rf = 0.49579376, chi^2 =  0.09394200, p-value = 0.75922429
bit  3:  rf = 0.49580764, chi^2 =  0.16832236, p-value = 0.68160710
bit  4:  rf = 0.49563340, chi^2 =  0.79701427, p-value = 0.37198755
bit  5:  rf = 0.49562675, chi^2 =  0.88831132, p-value = 0.34593534

modular monobit test for block length L = 7:
bit  0:  rf = 0.49552556, chi^2 =  2.47498722, p-value = 0.11567038
bit  1:  rf = 0.49606162, chi^2 =  4.57250003, p-value = 0.03248912
bit  2:  rf = 0.49574035, chi^2 =  0.00740412, p-value = 0.93142892
bit  3:  rf = 0.49563053, chi^2 =  0.71636473, p-value = 0.39733894
bit  4:  rf = 0.49581144, chi^2 =  0.16500407, p-value = 0.68459057
bit  5:  rf = 0.49586877, chi^2 =  0.64501800, p-value = 0.42189953
bit  6:  rf = 0.49563120, chi^2 =  0.70856195, p-value = 0.39992162

modular monobit test for block length L = 8:
bit  0:  rf = 0.49624176, chi^2 = 10.02955303, p-value = 0.00154048
bit  1:  rf = 0.49560127, chi^2 =  0.96279583, p-value = 0.32648347
bit  2:  rf = 0.49577503, chi^2 =  0.02077782, p-value = 0.88538585
bit  3:  rf = 0.49586134, chi^2 =  0.49438139, p-value = 0.48197935
bit  4:  rf = 0.49556227, chi^2 =  1.52236694, p-value = 0.21726166
bit  5:  rf = 0.49575329, chi^2 =  0.00001102, p-value = 0.99735111
bit  6:  rf = 0.49553547, chi^2 =  1.98078406, p-value = 0.15930783
bit  7:  rf = 0.49569178, chi^2 =  0.15607821, p-value = 0.69279318

modular monobit test for block length L = 9:
bit  0:  rf = 0.49589145, chi^2 =  0.71697412, p-value = 0.39713825
bit  1:  rf = 0.49581409, chi^2 =  0.14017574, p-value = 0.70810637
bit  2:  rf = 0.49603929, chi^2 =  3.06075355, p-value = 0.08020447
bit  3:  rf = 0.49555435, chi^2 =  1.46809359, p-value = 0.22564672
bit  4:  rf = 0.49581194, chi^2 =  0.13053629, p-value = 0.71787664
bit  5:  rf = 0.49557634, chi^2 =  1.16068124, p-value = 0.28132430
bit  6:  rf = 0.49612877, chi^2 =  5.27103024, p-value = 0.02168318
bit  7:  rf = 0.49544362, chi^2 =  3.56354234, p-value = 0.05906157
bit  8:  rf = 0.49551519, chi^2 =  2.10472936, p-value = 0.14684432

modular monobit test for block length L = 10:
bit  0:  rf = 0.49550819, chi^2 =  2.00737793, p-value = 0.15653566
bit  1:  rf = 0.49567068, chi^2 =  0.22618385, p-value = 0.63436800
bit  2:  rf = 0.49604535, chi^2 =  2.87247808, p-value = 0.09010603
bit  3:  rf = 0.49570763, chi^2 =  0.06838991, p-value = 0.79369565
bit  4:  rf = 0.49579549, chi^2 =  0.06122024, p-value = 0.80457759
bit  5:  rf = 0.49596667, chi^2 =  1.53529397, p-value = 0.21531965
bit  6:  rf = 0.49569643, chi^2 =  0.10655471, p-value = 0.74410117
bit  7:  rf = 0.49574947, chi^2 =  0.00036590, p-value = 0.98473861
bit  8:  rf = 0.49584770, chi^2 =  0.30238125, p-value = 0.58239343
bit  9:  rf = 0.49554014, chi^2 =  1.51720775, p-value = 0.21804253
```

```
**********************************************************************
*                                                                    *
*                 Results of the autocorrelation test                *
*                                                                    *
**********************************************************************


test scope:     first 10000000 bytes
relative frequency of bit 1:  0.49574462

bit shift d =  1:  chi^2 =  0.24270130,  p-value = 0.62226186
bit shift d =  2:  chi^2 =  2.04628173,  p-value = 0.15257843
bit shift d =  3:  chi^2 =  0.00094964,  p-value = 0.97541607
bit shift d =  4:  chi^2 =  0.07084243,  p-value = 0.79011413
bit shift d =  5:  chi^2 =  0.39513824,  p-value = 0.52961082
bit shift d =  6:  chi^2 =  0.34935558,  p-value = 0.55447815
bit shift d =  7:  chi^2 =  1.13755656,  p-value = 0.28616923
bit shift d =  8:  chi^2 =  1.65963732,  p-value = 0.19765230
bit shift d =  9:  chi^2 =  0.34091458,  p-value = 0.55930178
bit shift d = 10:  chi^2 =  3.15351903,  p-value = 0.07576341


**********************************************************************
*                                                                    *
*                   Results of the dependency test                   *
*                                                                    *
**********************************************************************


test scope:     first 10485760 bytes
relative frequency of bit 1:  0.49575278

dependency test for block length L = 3:

bit place 1 if bit 0 = 0:
rf = 0.49567903, chi^2 =  0.30670246, p-value = 0.57971077
bit place 1 if bit 0 = 1:
rf = 0.49570093, chi^2 =  0.14910405, p-value = 0.69939303
bit place 2 if bit 1 = 0:
rf = 0.49569323, chi^2 =  0.19998670, p-value = 0.65473158
bit place 2 if bit 1 = 1:
rf = 0.49572761, chi^2 =  0.03512829, p-value = 0.85132708
bit place 3 if bit 2 = 0:
rf = 0.49584014, chi^2 =  0.43055434, p-value = 0.51171707
bit place 3 if bit 2 = 1:
rf = 0.49587654, chi^2 =  0.84937315, p-value = 0.35672973

dependency test for block length L = 4:

bit place 1 if bit 0 = 0:
rf = 0.49575243, chi^2 =  0.00000495, p-value = 0.99822399
bit place 1 if bit 0 = 1:
rf = 0.49560093, chi^2 =  0.95918959, p-value = 0.32739115
bit place 2 if bit 1 = 0:
rf = 0.49553332, chi^2 =  2.03770422, p-value = 0.15344107
bit place 2 if bit 1 = 1:
rf = 0.49577936, chi^2 =  0.02938815, p-value = 0.86388588
bit place 3 if bit 2 = 0:
rf = 0.49572468, chi^2 =  0.03339287, p-value = 0.85500426
bit place 3 if bit 2 = 1:
rf = 0.49582929, chi^2 =  0.24346492, p-value = 0.62171469
bit place 4 if bit 3 = 0:
rf = 0.49593951, chi^2 =  1.47495620, p-value = 0.22456534
bit place 4 if bit 3 = 1:
rf = 0.49586383, chi^2 =  0.51298300, p-value = 0.47385038

dependency test for block length L = 5:

bit place 1 if bit 0 = 0:
rf = 0.49562122, chi^2 =  0.58570231, p-value = 0.44408584
bit place 1 if bit 0 = 1:
rf = 0.49574701, chi^2 =  0.00110540, p-value = 0.97347715
bit place 2 if bit 1 = 0:
rf = 0.49590753, chi^2 =  0.81057639, p-value = 0.36794990
bit place 2 if bit 1 = 1:
rf = 0.49588718, chi^2 =  0.60094742, p-value = 0.43821677
bit place 3 if bit 2 = 0:
```

```
rf = 0.49573257, chi^2 =  0.01380934, p-value = 0.90645342
bit place 3 if bit 2 = 1:
rf = 0.49582357, chi^2 =  0.16678478, p-value = 0.68298522
bit place 4 if bit 3 = 0:
rf = 0.49578388, chi^2 =  0.03274954, p-value = 0.85639242
bit place 4 if bit 3 = 1:
rf = 0.49554971, chi^2 =  1.37207964, p-value = 0.24145489
bit place 5 if bit 4 = 0:
rf = 0.49564215, chi^2 =  0.41419939, p-value = 0.51984572
bit place 5 if bit 4 = 1:
rf = 0.49583432, chi^2 =  0.22119075, p-value = 0.63813412

dependency test for block length L = 6:

bit place 1 if bit 0 = 0:
rf = 0.49586965, chi^2 =  0.38509248, p-value = 0.53489035
bit place 1 if bit 0 = 1:
rf = 0.49562092, chi^2 =  0.48219606, p-value = 0.48742927
bit place 2 if bit 1 = 0:
rf = 0.49583112, chi^2 =  0.17310394, p-value = 0.67736785
bit place 2 if bit 1 = 1:
rf = 0.49575568, chi^2 =  0.00023458, p-value = 0.98778001
bit place 3 if bit 2 = 0:
rf = 0.49579065, chi^2 =  0.04045995, p-value = 0.84058395
bit place 3 if bit 2 = 1:
rf = 0.49582483, chi^2 =  0.14397319, p-value = 0.70436264
bit place 4 if bit 3 = 0:
rf = 0.49548837, chi^2 =  1.97132327, p-value = 0.16030747
bit place 4 if bit 3 = 1:
rf = 0.49578095, chi^2 =  0.02201130, p-value = 0.88205705
bit place 5 if bit 4 = 0:
rf = 0.49555538, chi^2 =  1.09916391, p-value = 0.29444966
bit place 5 if bit 4 = 1:
rf = 0.49569945, chi^2 =  0.07883496, p-value = 0.77888249
bit place 6 if bit 5 = 0:
rf = 0.49588961, chi^2 =  0.52819366, p-value = 0.46736727
bit place 6 if bit 5 = 1:
rf = 0.49592820, chi^2 =  0.85300813, p-value = 0.35570274

dependency test for block length L = 7:

bit place 1 if bit 0 = 0:
rf = 0.49611007, chi^2 =  3.08728605, p-value = 0.07890631
bit place 1 if bit 0 = 1:
rf = 0.49601220, chi^2 =  1.59874943, p-value = 0.20608052
bit place 2 if bit 1 = 0:
rf = 0.49587610, chi^2 =  0.36739180, p-value = 0.54442940
bit place 2 if bit 1 = 1:
rf = 0.49560236, chi^2 =  0.53803210, p-value = 0.46324943
bit place 3 if bit 2 = 0:
rf = 0.49565317, chi^2 =  0.23983259, p-value = 0.62432705
bit place 3 if bit 2 = 1:
rf = 0.49560742, chi^2 =  0.50210682, p-value = 0.47857586
bit place 4 if bit 3 = 0:
rf = 0.49559902, chi^2 =  0.57158623, p-value = 0.44962928
bit place 4 if bit 3 = 1:
rf = 0.49602770, chi^2 =  1.79577755, p-value = 0.18022381
bit place 5 if bit 4 = 0:
rf = 0.49592556, chi^2 =  0.72157310, p-value = 0.39562839
bit place 5 if bit 4 = 1:
rf = 0.49581094, chi^2 =  0.08041232, p-value = 0.77673942
bit place 6 if bit 5 = 0:
rf = 0.49563725, chi^2 =  0.32255217, p-value = 0.57007791
bit place 6 if bit 5 = 1:
rf = 0.49562497, chi^2 =  0.38830803, p-value = 0.53319012
bit place 7 if bit 6 = 0:
rf = 0.49536110, chi^2 =  3.70917969, p-value = 0.05411398
bit place 7 if bit 6 = 1:
rf = 0.49569282, chi^2 =  0.08539637, p-value = 0.77011340

dependency test for block length L = 8:

bit place 1 if bit 0 = 0:
rf = 0.49576594, chi^2 =  0.00366405, p-value = 0.95173238
bit place 1 if bit 0 = 1:
rf = 0.49543401, chi^2 =  2.11508122, p-value = 0.14585432
bit place 2 if bit 1 = 0:
rf = 0.49579713, chi^2 =  0.04162204, p-value = 0.83834193
```

```
bit place 2 if bit 1 = 1:
rf = 0.49575245, chi^2 =  0.00000227, p-value = 0.99879894
bit place 3 if bit 2 = 0:
rf = 0.49597536, chi^2 =  1.04787105, p-value = 0.30599791
bit place 3 if bit 2 = 1:
rf = 0.49574528, chi^2 =  0.00116904, p-value = 0.97272465
bit place 4 if bit 3 = 0:
rf = 0.49570615, chi^2 =  0.04597906, p-value = 0.83021386
bit place 4 if bit 3 = 1:
rf = 0.49541608, chi^2 =  2.35788023, p-value = 0.12465147
bit place 5 if bit 4 = 0:
rf = 0.49573885, chi^2 =  0.00410574, p-value = 0.94890970
bit place 5 if bit 4 = 1:
rf = 0.49576808, chi^2 =  0.00487179, p-value = 0.94435425
bit place 6 if bit 5 = 0:
rf = 0.49526942, chi^2 =  4.94155962, p-value = 0.02621837
bit place 6 if bit 5 = 1:
rf = 0.49580617, chi^2 =  0.05928368, p-value = 0.80763171
bit place 7 if bit 6 = 0:
rf = 0.49547412, chi^2 =  1.64304054, p-value = 0.19990880
bit place 7 if bit 6 = 1:
rf = 0.49591325, chi^2 =  0.53530439, p-value = 0.46438528
bit place 8 if bit 7 = 0:
rf = 0.49617279, chi^2 =  3.73176535, p-value = 0.05338694
bit place 8 if bit 7 = 1:
rf = 0.49631183, chi^2 =  6.49853820, p-value = 0.01079632

dependency test for block length L = 9:

bit place 1 if bit 0 = 0:
rf = 0.49583102, chi^2 =  0.11507084, p-value = 0.73444330
bit place 1 if bit 0 = 1:
rf = 0.49579699, chi^2 =  0.03614277, p-value = 0.84922096
bit place 2 if bit 1 = 0:
rf = 0.49591646, chi^2 =  0.50365638, p-value = 0.47789793
bit place 2 if bit 1 = 1:
rf = 0.49616408, chi^2 =  3.12747569, p-value = 0.07698286
bit place 3 if bit 2 = 0:
rf = 0.49553484, chi^2 =  0.89248294, p-value = 0.34480534
bit place 3 if bit 2 = 1:
rf = 0.49557406, chi^2 =  0.59074693, p-value = 0.44213043
bit place 4 if bit 3 = 0:
rf = 0.49580797, chi^2 =  0.05728847, p-value = 0.81083411
bit place 4 if bit 3 = 1:
rf = 0.49581589, chi^2 =  0.07359413, p-value = 0.78617386
bit place 5 if bit 4 = 0:
rf = 0.49572039, chi^2 =  0.01972105, p-value = 0.88831894
bit place 5 if bit 4 = 1:
rf = 0.49542975, chi^2 =  1.92898626, p-value = 0.16486940
bit place 6 if bit 5 = 0:
rf = 0.49605972, chi^2 =  1.77195363, p-value = 0.18314049
bit place 6 if bit 5 = 1:
rf = 0.49619916, chi^2 =  3.68178328, p-value = 0.05500999
bit place 7 if bit 6 = 0:
rf = 0.49539788, chi^2 =  2.36629019, p-value = 0.12398137
bit place 7 if bit 6 = 1:
rf = 0.49548998, chi^2 =  1.27756203, p-value = 0.25835283
bit place 8 if bit 7 = 0:
rf = 0.49544293, chi^2 =  1.80604943, p-value = 0.17898287
bit place 8 if bit 7 = 1:
rf = 0.49558866, chi^2 =  0.49756427, p-value = 0.48057232
bit place 9 if bit 8 = 0:
rf = 0.49592558, chi^2 =  0.56167420, p-value = 0.45358647
bit place 9 if bit 8 = 1:
rf = 0.49585659, chi^2 =  0.19910464, p-value = 0.65544452

dependency test for block length L = 10:

bit place 1 if bit 0 = 0:
rf = 0.49564483, chi^2 =  0.19725465, p-value = 0.65694600
bit place 1 if bit 0 = 1:
rf = 0.49569687, chi^2 =  0.05197378, p-value = 0.81966367
bit place 2 if bit 1 = 0:
rf = 0.49593759, chi^2 =  0.57807700, p-value = 0.44706707
bit place 2 if bit 1 = 1:
rf = 0.49615511, chi^2 =  2.69245162, p-value = 0.10082458
bit place 3 if bit 2 = 0:
rf = 0.49582056, chi^2 =  0.07769449, p-value = 0.78044643
```

```
bit place 3 if bit 2 = 1:
rf = 0.49559278, chi^2 =  0.42608773, p-value = 0.51391491
bit place 4 if bit 3 = 0:
rf = 0.49595857, chi^2 =  0.71669803, p-value = 0.39722916
bit place 4 if bit 3 = 1:
rf = 0.49562946, chi^2 =  0.25295598, p-value = 0.61500133
bit place 5 if bit 4 = 0:
rf = 0.49574071, chi^2 =  0.00246486, p-value = 0.96040338
bit place 5 if bit 4 = 1:
rf = 0.49619635, chi^2 =  3.27355221, p-value = 0.07040502
bit place 6 if bit 5 = 0:
rf = 0.49559759, chi^2 =  0.40733119, p-value = 0.52332721
bit place 6 if bit 5 = 1:
rf = 0.49579699, chi^2 =  0.03253313, p-value = 0.85686256
bit place 7 if bit 6 = 0:
rf = 0.49587746, chi^2 =  0.26309519, p-value = 0.60800164
bit place 7 if bit 6 = 1:
rf = 0.49561938, chi^2 =  0.29598463, p-value = 0.58641072
bit place 8 if bit 7 = 0:
rf = 0.49564452, chi^2 =  0.19830119, p-value = 0.65609558
bit place 8 if bit 7 = 1:
rf = 0.49605449, chi^2 =  1.51435103, p-value = 0.21847636
bit place 9 if bit 8 = 0:
rf = 0.49560915, chi^2 =  0.34898817, p-value = 0.55468646
bit place 9 if bit 8 = 1:
rf = 0.49546986, chi^2 =  1.33183542, p-value = 0.24847896
bit place 10 if bit 9 = 0:
rf = 0.49554365, chi^2 =  0.74031249, p-value = 0.38956080
bit place 10 if bit 9 = 1:
rf = 0.49547198, chi^2 =  1.31114735, p-value = 0.25218703
```

4 AIS31 evaluation tests kurz bei -40°C

```
**************************************************************************
*                                                                        *
*                        AIS31 evaluation tests                          *
*                                                                        *
**************************************************************************


date, time:     06/13/2019,  18:25:12
tested file:    T-40.rnd
size of file:   10485760 bytes


--------------------------------------------------------------------------
Introduction
--------------------------------------------------------------------------

The purpose of the following tests is to evaluate the suitability
of a true (physical) random number generator for cryptographic
applications. In [1] an evaluation methodology for physical random
number generators has been proposed by the German Federal Security
Agency. In the mathematical-technical reference to [1], five tests
are defined for the P2-evaluation of a physical random number
generator (cf. [3] and [4]) which are implemented in the following
tests 1 - 5.


--------------------------------------------------------------------------
Results of test 1  (test (P2.i)(vii.a) of AIS 31, cf. [3] and [4])
--------------------------------------------------------------------------

In this test, the relative frequency r of bit 1 ocurring in the
first 100000 bits of the bit sequence is computed. Then the bit
sequence passes the test if |r - 0.5| < 0.025.

test scope:  first 100000 bits
number of ones:  49518
relative frequency:  0.495180
test value:  0.00482000  < 0.025
```

```
sequence passes test 1


------------------------------------------------------------------------
Results of test 2  (test (P2.i)(vii.b) of AIS 31, cf. [3] and [4])
------------------------------------------------------------------------

In this test, two disjoint sub-sequences TF(0) and TF(1) of bit pairs
are considered where TF(i) consists of the first 100000 bit pairs
of the form (i,x) ocurring in the bit sequence after the test scope
of test 1. Let v(i,j) denote the relative frequency of all bit pairs
of the form (i,j) in TF(i). Then the bit sequence passes the test
if |v(0,1) + v(1,0) - 1| < 0.02.

number of 2-bit words looked up: 201324
relative frequency v(0,1):  0.495600
relative frequency v(1,0):  0.504450
test value:  0.00005000 < 0.02

sequence passes test 2


------------------------------------------------------------------------
Results of test 3  (test (P2.i)(vii.c) of AIS 31, cf. [3] and [4])
------------------------------------------------------------------------

In this test, 4 disjoint sub-sequences TF(0,0),..., TF(1,1) of
3-tupels are considered where TF(i,j) consists of the first 100000
3-tupels of bits of the form (i,j,x) ocurring in the bit sequence
after the test scope of test 2. For every i,j in {0,1}, let S(i,j)
denote the sub-sequence of all bits k such that (i,j,k) is element
of TF(i,j). Then sample S(0,j) is compared with S(1,j) for every
j = 0,1. In this context, a comparison of two bit sequences g and h
of equal length is performed by a computation of the test value
t = (g_0 - h_0)^2 /(g_0 + h_0) + (g_1 - h_1)^2 /(g_1 + h_1) where
g_i resp. h_i is the number of bit i occurring in sequence g resp. h.
Let t_j be the test value for the comparison of S(0,j) with S(1,j)
Then the bit sequence passes the test if t_j < 15,13 for j = 0,1.

number of 3-bit words looked up: 408560
test value t_1:    0.486784 <= 15.13
test value t_2:    4.213962 <= 15.13

sequence passes test 3


------------------------------------------------------------------------
Results of test 4  (test (P2.i)(vii.d) of AIS 31, cf. [3] and [4])
------------------------------------------------------------------------

In this test, 8 disjoint sub-sequences TF(0,0,0),..., TF(1,1,1) of
4-tupels are considered where TF(i,j,k) consists of the first 100000
4-tupels of bits of the form (i,j,k,x) ocurring in the bit sequence
after the test scope of test 3. For every i,j in {0,1}, let S(i,j,k)
denote the sub-sequence of all bits b such that (i,j,k,b) is  an
element of TF(i,j,k). Then sample S(0,j,k) is compared with S(1,j,k)
for every j,k of {0,1}. In this context, a comparison of two bit
sequences g and h of equal length is performed by a computation of the
test value t = (g_0 - h_0)^2 /(g_0 + h_0) + (g_1 - h_1)^2 /(g_1 + h_1)
where g_i resp. h_i is the number of bit i occurring in sequence g
resp. h. Let t_jk be the test value for the comparison of S(0,j,k)
with S(1,j,k). Then the bit sequence passes the test if t_jk < 15,13
for all j,k of {0,1}.

number of 4-bit words looked up: 819036
test value t_00:    0.052025 <= 15.13
test value t_01:    0.699408 <= 15.13
test value t_10:    0.444060 <= 15.13
test value t_11:    0.000000 <= 15.13

sequence passes test 4


------------------------------------------------------------------------
Results of test 5  (test (P2.i)(vii.e) of AIS 31, cf. [3] and [4])
------------------------------------------------------------------------

In this test, the Coron test with the parameters L = 8, Q = 2560,
```

```
and K = 256000 is performed (cf. [2]). For the first Q+K 8-bit-words
after the test scope of test 4, the test value f of the Coron test is
computed. The bit sequence passes the test if f > 7.976.

8-bit words looked up: 2560 + 256000 bytes
f-value:  8.00222019
8.00222019 > 7.976

sequence passes test 5

------------------------------------------------------------------------
References
------------------------------------------------------------------------

[1]  AIS 31: Functionality Classes and Evaluation Methodology for
     Physical Random Number Generators. Version 1 (25.09.2001),
     (mandatory if a German IT security certificate is applied for;
     English translation).
     available at www.bsi.bund.de/zertifiz/zert/interpr/ais31e.pdf

[2]  J.- S. Coron: On the Security of Random Sources. In: Public Key
     Cryptography - PKC 99. Lecture Notes in Computer Science,
     Vol. 1560, 29-42, Springer-Verlag, 2002.

[3]  W. Killmann and W. Schindler: A Proposal for: Functionality
     Classes and Evaluation Methodology for True (Physical) Random
     Number Generators. Version 3.1 (25.09.2001), mathematical-
     technical reference of [1] (English Translation);
     available at www.bsi.bund.de/zertifiz/zert/interpr/trngk31e.pdf

[4]  W. Schindler and W. Killmann: Evaluation Criteria for True
     (Physical) Random Number Generators Used in Cryptographic
     Applications. In: Cryptographic Hardware and Empedded  Systems
     - CHES 2002. Lecture Notes in Computer Science, Vol. 2523,
     431-449, Springer-Verlag, 2002.
```

5 AIS31 evaluation tests lang bei -40°C

```
###########################################################################
#                                                                         #
#                          Results of RawTest                             #
#                                                                         #
###########################################################################


date, time:    06/13/2019,  18:25:26
tested file:   T-40.rnd
size of file:  10485760 bytes


***************************************************************************
*                                                                         *
*                    Results of the frequency test                        *
*                                                                         *
***************************************************************************


test scope:     first 10485760 bytes
relative frequency of bit 1:  0.49594426

block length L =  2:  chi^2 =     0.4806,  p-value = 0.92313222
block length L =  3:  chi^2 =     4.0679,  p-value = 0.77192239
block length L =  4:  chi^2 =    17.9326,  p-value = 0.26622303
block length L =  5:  chi^2 =    23.3336,  p-value = 0.83676540
block length L =  6:  chi^2 =    52.4582,  p-value = 0.82562245
block length L =  7:  chi^2 =   145.3770,  p-value = 0.12650072
block length L =  8:  chi^2 =   239.9138,  p-value = 0.74279971
block length L =  9:  chi^2 =   483.9383,  p-value = 0.79981958
block length L = 10:  chi^2 =  1012.6839,  p-value = 0.58476039


***************************************************************************
```

```
*                                                                     *
*                      Results of the serial test                     *
*                                                                     *
***********************************************************************


test scope:     first 10000000 bytes
relative frequency of bit 1:  0.49595211

block length L =  2:  chi^2 =     0.2109,  p-value = 0.89993001
block length L =  3:  chi^2 =     0.3392,  p-value = 0.98714226
block length L =  4:  chi^2 =     4.3325,  p-value = 0.82594780
block length L =  5:  chi^2 =    14.7132,  p-value = 0.54573886
block length L =  6:  chi^2 =    29.5369,  p-value = 0.59179676
block length L =  7:  chi^2 =    71.6339,  p-value = 0.23945639
block length L =  8:  chi^2 =   132.6885,  p-value = 0.37029137
block length L =  9:  chi^2 =   275.9223,  p-value = 0.18730414
block length L = 10:  chi^2 =   502.7460,  p-value = 0.60645097


***********************************************************************
*                                                                     *
*                Results of the modular monobit test                  *
*                                                                     *
***********************************************************************


test scope:     first 10485760 bytes
relative frequency of bit 1:  0.49594426

modular monobit test for block length L = 3:
bit  0:  rf = 0.49584125, chi^2 =  1.18687846, p-value = 0.27596011
bit  1:  rf = 0.49598169, chi^2 =  0.15672363, p-value = 0.69219108
bit  2:  rf = 0.49600980, chi^2 =  0.48049139, p-value = 0.48819982

modular monobit test for block length L = 4:
bit  0:  rf = 0.49607015, chi^2 =  1.32943317, p-value = 0.24890608
bit  1:  rf = 0.49597254, chi^2 =  0.06707614, p-value = 0.79564248
bit  2:  rf = 0.49586258, chi^2 =  0.55972330, p-value = 0.45437175
bit  3:  rf = 0.49587178, chi^2 =  0.44070282, p-value = 0.50678343

modular monobit test for block length L = 5:
bit  0:  rf = 0.49589694, chi^2 =  0.15031755, p-value = 0.69823208
bit  1:  rf = 0.49600333, chi^2 =  0.23416176, p-value = 0.62845497
bit  2:  rf = 0.49589133, chi^2 =  0.18801591, p-value = 0.66457311
bit  3:  rf = 0.49588662, chi^2 =  0.22295726, p-value = 0.63679581
bit  4:  rf = 0.49604309, chi^2 =  0.65544722, p-value = 0.41817186

modular monobit test for block length L = 6:
bit  0:  rf = 0.49578382, chi^2 =  1.43970508, p-value = 0.23018707
bit  1:  rf = 0.49589411, chi^2 =  0.14066762, p-value = 0.70761821
bit  2:  rf = 0.49604596, chi^2 =  0.57842424, p-value = 0.44693063
bit  3:  rf = 0.49589869, chi^2 =  0.11616034, p-value = 0.73323681
bit  4:  rf = 0.49606928, chi^2 =  0.87407619, p-value = 0.34982931
bit  5:  rf = 0.49597365, chi^2 =  0.04829236, p-value = 0.82606179

modular monobit test for block length L = 7:
bit  0:  rf = 0.49603767, chi^2 =  0.41824604, p-value = 0.51781354
bit  1:  rf = 0.49591901, chi^2 =  0.03057496, p-value = 0.86119202
bit  2:  rf = 0.49601923, chi^2 =  0.26939652, p-value = 0.60373688
bit  3:  rf = 0.49591308, chi^2 =  0.04660332, p-value = 0.82908283
bit  4:  rf = 0.49599352, chi^2 =  0.11633814, p-value = 0.73304052
bit  5:  rf = 0.49575470, chi^2 =  1.72257424, p-value = 0.18936202
bit  6:  rf = 0.49597258, chi^2 =  0.03844176, p-value = 0.84455873

modular monobit test for block length L = 8:
bit  0:  rf = 0.49621668, chi^2 =  3.11284224, p-value = 0.07767730
bit  1:  rf = 0.49586258, chi^2 =  0.27986165, p-value = 0.59679191
bit  2:  rf = 0.49604282, chi^2 =  0.40748311, p-value = 0.52324975
bit  3:  rf = 0.49588852, chi^2 =  0.13033399, p-value = 0.71808600
bit  4:  rf = 0.49592361, chi^2 =  0.01788152, p-value = 0.89362256
bit  5:  rf = 0.49608250, chi^2 =  0.80153980, p-value = 0.37063339
bit  6:  rf = 0.49568233, chi^2 =  2.87771553, p-value = 0.08981336
bit  7:  rf = 0.49585505, chi^2 =  0.33386911, p-value = 0.56338965

modular monobit test for block length L = 9:
bit  0:  rf = 0.49602180, chi^2 =  0.22417197, p-value = 0.63587931
```

```
bit  1:  rf = 0.49585229, chi^2 =  0.31541810, p-value = 0.57437430
bit  2:  rf = 0.49584789, chi^2 =  0.34630973, p-value = 0.55620957
bit  3:  rf = 0.49587160, chi^2 =  0.19686919, p-value = 0.65725991
bit  4:  rf = 0.49593779, chi^2 =  0.00155951, p-value = 0.96849922
bit  5:  rf = 0.49613467, chi^2 =  1.35176399, p-value = 0.24496997
bit  6:  rf = 0.49563041, chi^2 =  3.67262085, p-value = 0.05531314
bit  7:  rf = 0.49615495, chi^2 =  1.65500883, p-value = 0.19827857
bit  8:  rf = 0.49604691, chi^2 =  0.39283564, p-value = 0.53081262

modular monobit test for block length L = 10:
bit  0:  rf = 0.49584997, chi^2 =  0.29836758, p-value = 0.58490761
bit  1:  rf = 0.49586713, chi^2 =  0.19962146, p-value = 0.65502657
bit  2:  rf = 0.49590588, chi^2 =  0.04944364, p-value = 0.82403423
bit  3:  rf = 0.49587154, chi^2 =  0.17744278, p-value = 0.67358015
bit  4:  rf = 0.49603474, chi^2 =  0.27471490, p-value = 0.60018637
bit  5:  rf = 0.49594390, chi^2 =  0.00000429, p-value = 0.99834705
bit  6:  rf = 0.49613953, chi^2 =  1.27945926, p-value = 0.25799960
bit  7:  rf = 0.49587679, chi^2 =  0.15276770, p-value = 0.69590436
bit  8:  rf = 0.49590170, chi^2 =  0.06077642, p-value = 0.80527296
bit  9:  rf = 0.49605143, chi^2 =  0.38540563, p-value = 0.53472434



*************************************************************************
*                                                                       *
*                 Results of the autocorrelation test                   *
*                                                                       *
*************************************************************************


test scope:     first 10000000 bytes
relative frequency of bit 1:  0.49595211

bit shift d =  1:  chi^2 =  0.21077389,  p-value = 0.64616151
bit shift d =  2:  chi^2 =  0.02558536,  p-value = 0.87291711
bit shift d =  3:  chi^2 =  0.17939265,  p-value = 0.67189571
bit shift d =  4:  chi^2 =  1.12781026,  p-value = 0.28824290
bit shift d =  5:  chi^2 =  4.51740625,  p-value = 0.03355166
bit shift d =  6:  chi^2 =  0.21910307,  p-value = 0.63972419
bit shift d =  7:  chi^2 =  2.34281282,  p-value = 0.12586210
bit shift d =  8:  chi^2 =  0.85064219,  p-value = 0.35637073
bit shift d =  9:  chi^2 =  3.48459136,  p-value = 0.06194265
bit shift d = 10:  chi^2 =  0.51338898,  p-value = 0.47367546



*************************************************************************
*                                                                       *
*                   Results of the dependency test                      *
*                                                                       *
*************************************************************************


test scope:     first 10485760 bytes
relative frequency of bit 1:  0.49594426

dependency test for block length L = 3:

bit place 1 if bit 0 = 0:
rf = 0.49608914, chi^2 =  1.18374661, p-value = 0.27659458
bit place 1 if bit 0 = 1:
rf = 0.49587240, chi^2 =  0.28638846, p-value = 0.59254424
bit place 2 if bit 1 = 0:
rf = 0.49603037, chi^2 =  0.41800171, p-value = 0.51793584
bit place 2 if bit 1 = 1:
rf = 0.49598894, chi^2 =  0.11074201, p-value = 0.73930095
bit place 3 if bit 2 = 0:
rf = 0.49580893, chi^2 =  1.03245425, p-value = 0.30958293
bit place 3 if bit 2 = 1:
rf = 0.49587406, chi^2 =  0.27344175, p-value = 0.60103230

dependency test for block length L = 4:

bit place 1 if bit 0 = 0:
rf = 0.49592555, chi^2 =  0.01480149, p-value = 0.90316721
bit place 1 if bit 0 = 1:
rf = 0.49602032, chi^2 =  0.24073241, p-value = 0.62367763
bit place 2 if bit 1 = 0:
```

```
rf = 0.49598093, chi^2 =  0.05684128, p-value = 0.81155994
bit place 2 if bit 1 = 1:
rf = 0.49574226, chi^2 =  1.69775959, p-value = 0.19258123
bit place 3 if bit 2 = 0:
rf = 0.49583260, chi^2 =  0.52736240, p-value = 0.46771788
bit place 3 if bit 2 = 1:
rf = 0.49591157, chi^2 =  0.04444586, p-value = 0.83302628
bit place 4 if bit 3 = 0:
rf = 0.49616561, chi^2 =  2.07202967, p-value = 0.15002175
bit place 4 if bit 3 = 1:
rf = 0.49597305, chi^2 =  0.03447522, p-value = 0.85269961

dependency test for block length L = 5:

bit place 1 if bit 0 = 0:
rf = 0.49607417, chi^2 =  0.57094684, p-value = 0.44988291
bit place 1 if bit 0 = 1:
rf = 0.49593126, chi^2 =  0.00562785, p-value = 0.94019957
bit place 2 if bit 1 = 0:
rf = 0.49585301, chi^2 =  0.28162409, p-value = 0.59563870
bit place 2 if bit 1 = 1:
rf = 0.49593033, chi^2 =  0.00646326, p-value = 0.93592357
bit place 3 if bit 2 = 0:
rf = 0.49604170, chi^2 =  0.32119492, p-value = 0.57089043
bit place 3 if bit 2 = 1:
rf = 0.49572892, chi^2 =  1.54329801, p-value = 0.21412757
bit place 4 if bit 3 = 0:
rf = 0.49593544, chi^2 =  0.00263286, p-value = 0.95907737
bit place 4 if bit 3 = 1:
rf = 0.49615246, chi^2 =  1.44256354, p-value = 0.22972495
bit place 5 if bit 4 = 0:
rf = 0.49597646, chi^2 =  0.03506652, p-value = 0.85145633
bit place 5 if bit 4 = 1:
rf = 0.49581608, chi^2 =  0.54698227, p-value = 0.45955337

dependency test for block length L = 6:

bit place 1 if bit 0 = 0:
rf = 0.49609083, chi^2 =  0.60580595, p-value = 0.43637133
bit place 1 if bit 0 = 1:
rf = 0.49569397, chi^2 =  1.73704620, p-value = 0.18751353
bit place 2 if bit 1 = 0:
rf = 0.49625442, chi^2 =  2.71220159, p-value = 0.09958347
bit place 2 if bit 1 = 1:
rf = 0.49583412, chi^2 =  0.33647766, p-value = 0.56186947
bit place 3 if bit 2 = 0:
rf = 0.49574008, chi^2 =  1.17505377, p-value = 0.27836525
bit place 3 if bit 2 = 1:
rf = 0.49605990, chi^2 =  0.37096420, p-value = 0.54247916
bit place 4 if bit 3 = 0:
rf = 0.49608746, chi^2 =  0.57810119, p-value = 0.44705756
bit place 4 if bit 3 = 1:
rf = 0.49605072, chi^2 =  0.31433787, p-value = 0.57503042
bit place 5 if bit 4 = 0:
rf = 0.49580624, chi^2 =  0.53692379, p-value = 0.46371041
bit place 5 if bit 4 = 1:
rf = 0.49614378, chi^2 =  1.10443396, p-value = 0.29329509
bit place 6 if bit 5 = 0:
rf = 0.49587784, chi^2 =  0.12434974, p-value = 0.72436390
bit place 6 if bit 5 = 1:
rf = 0.49568819, chi^2 =  1.81887135, p-value = 0.17744768

dependency test for block length L = 7:

bit place 1 if bit 0 = 0:
rf = 0.49600329, chi^2 =  0.08418348, p-value = 0.77170616
bit place 1 if bit 0 = 1:
rf = 0.49583346, chi^2 =  0.29194170, p-value = 0.58897892
bit place 2 if bit 1 = 0:
rf = 0.49607409, chi^2 =  0.40731347, p-value = 0.52333624
bit place 2 if bit 1 = 1:
rf = 0.49596354, chi^2 =  0.00883685, p-value = 0.92510556
bit place 3 if bit 2 = 0:
rf = 0.49597007, chi^2 =  0.01609813, p-value = 0.89903665
bit place 3 if bit 2 = 1:
rf = 0.49585526, chi^2 =  0.18836119, p-value = 0.66428410
bit place 4 if bit 3 = 0:
rf = 0.49604989, chi^2 =  0.26959571, p-value = 0.60360310
```

```
bit place 4 if bit 3 = 1:
rf = 0.49593615, chi^2 =  0.00156438, p-value = 0.96845008
bit place 5 if bit 4 = 0:
rf = 0.49577251, chi^2 =  0.71270287, p-value = 0.39854798
bit place 5 if bit 4 = 1:
rf = 0.49573652, chi^2 =  1.02616265, p-value = 0.31106166
bit place 6 if bit 5 = 0:
rf = 0.49586868, chi^2 =  0.13809930, p-value = 0.71017793
bit place 6 if bit 5 = 1:
rf = 0.49607835, chi^2 =  0.42726667, p-value = 0.51333321
bit place 7 if bit 6 = 0:
rf = 0.49609487, chi^2 =  0.54803426, p-value = 0.45912201
bit place 7 if bit 6 = 1:
rf = 0.49597946, chi^2 =  0.02945044, p-value = 0.86374312

dependency test for block length L = 8:

bit place 1 if bit 0 = 0:
rf = 0.49587519, chi^2 =  0.10080568, p-value = 0.75086492
bit place 1 if bit 0 = 1:
rf = 0.49584968, chi^2 =  0.18621345, p-value = 0.66608700
bit place 2 if bit 1 = 0:
rf = 0.49618805, chi^2 =  1.25674214, p-value = 0.26226866
bit place 2 if bit 1 = 1:
rf = 0.49589527, chi^2 =  0.04991296, p-value = 0.82321480
bit place 3 if bit 2 = 0:
rf = 0.49592241, chi^2 =  0.01009247, p-value = 0.91997810
bit place 3 if bit 2 = 1:
rf = 0.49585418, chi^2 =  0.16883428, p-value = 0.68114991
bit place 4 if bit 3 = 0:
rf = 0.49597322, chi^2 =  0.01773761, p-value = 0.89404895
bit place 4 if bit 3 = 1:
rf = 0.49587309, chi^2 =  0.10537682, p-value = 0.74547023
bit place 5 if bit 4 = 0:
rf = 0.49597588, chi^2 =  0.02113437, p-value = 0.88441350
bit place 5 if bit 4 = 1:
rf = 0.49619096, chi^2 =  1.26605062, p-value = 0.26050889
bit place 6 if bit 5 = 0:
rf = 0.49577372, chi^2 =  0.61478861, p-value = 0.43299049
bit place 6 if bit 5 = 1:
rf = 0.49558941, chi^2 =  2.62016310, p-value = 0.10551360
bit place 7 if bit 6 = 0:
rf = 0.49574294, chi^2 =  0.85739763, p-value = 0.35446797
bit place 7 if bit 6 = 1:
rf = 0.49596901, chi^2 =  0.01273344, p-value = 0.91015538
bit place 8 if bit 7 = 0:
rf = 0.49635788, chi^2 =  3.61777829, p-value = 0.05716516
bit place 8 if bit 7 = 1:
rf = 0.49607302, chi^2 =  0.34482444, p-value = 0.55705761

dependency test for block length L = 9:

bit place 1 if bit 0 = 0:
rf = 0.49595512, chi^2 =  0.00221452, p-value = 0.96246643
bit place 1 if bit 0 = 1:
rf = 0.49574769, chi^2 =  0.71458999, p-value = 0.39792424
bit place 2 if bit 1 = 0:
rf = 0.49587050, chi^2 =  0.10226652, p-value = 0.74912649
bit place 2 if bit 1 = 1:
rf = 0.49582500, chi^2 =  0.26295821, p-value = 0.60809507
bit place 3 if bit 2 = 0:
rf = 0.49572008, chi^2 =  0.94470271, p-value = 0.33107135
bit place 3 if bit 2 = 1:
rf = 0.49602576, chi^2 =  0.12279218, p-value = 0.72602566
bit place 4 if bit 3 = 0:
rf = 0.49597728, chi^2 =  0.02049786, p-value = 0.88615535
bit place 4 if bit 3 = 1:
rf = 0.49589775, chi^2 =  0.03999063, p-value = 0.84149891
bit place 5 if bit 4 = 0:
rf = 0.49600006, chi^2 =  0.05852090, p-value = 0.80884918
bit place 5 if bit 4 = 1:
rf = 0.49627159, chi^2 =  1.98116350, p-value = 0.15926789
bit place 6 if bit 5 = 0:
rf = 0.49585616, chi^2 =  0.14583351, p-value = 0.70254924
bit place 6 if bit 5 = 1:
rf = 0.49540104, chi^2 =  5.45863065, p-value = 0.01947190
bit place 7 if bit 6 = 0:
rf = 0.49633498, chi^2 =  2.87085566, p-value = 0.09019690
```

```
bit place 7 if bit 6 = 1:
rf = 0.49597163, chi^2 =  0.01384060, p-value = 0.90634808
bit place 8 if bit 7 = 0:
rf = 0.49622075, chi^2 =  1.43615859, p-value = 0.23076198
bit place 8 if bit 7 = 1:
rf = 0.49587047, chi^2 =  0.10072986, p-value = 0.75095553
bit place 9 if bit 8 = 0:
rf = 0.49585070, chi^2 =  0.16446998, p-value = 0.68507402
bit place 9 if bit 8 = 1:
rf = 0.49619552, chi^2 =  1.16758149, p-value = 0.27989874

dependency test for block length L = 10:

bit place 1 if bit 0 = 0:
rf = 0.49586722, chi^2 =  0.10040888, p-value = 0.75133951
bit place 1 if bit 0 = 1:
rf = 0.49586716, chi^2 =  0.09890671, p-value = 0.75314559
bit place 2 if bit 1 = 0:
rf = 0.49604656, chi^2 =  0.17702537, p-value = 0.67394216
bit place 2 if bit 1 = 1:
rf = 0.49576273, chi^2 =  0.54834254, p-value = 0.45899572
bit place 3 if bit 2 = 0:
rf = 0.49595213, chi^2 =  0.00104839, p-value = 0.97416996
bit place 3 if bit 2 = 1:
rf = 0.49578950, chi^2 =  0.39856010, p-value = 0.52783382
bit place 4 if bit 3 = 0:
rf = 0.49595265, chi^2 =  0.00118931, p-value = 0.97248934
bit place 4 if bit 3 = 1:
rf = 0.49611832, chi^2 =  0.50414079, p-value = 0.47768632
bit place 5 if bit 4 = 0:
rf = 0.49599864, chi^2 =  0.05001308, p-value = 0.82304052
bit place 5 if bit 4 = 1:
rf = 0.49588841, chi^2 =  0.05192558, p-value = 0.81974587
bit place 6 if bit 5 = 0:
rf = 0.49628127, chi^2 =  1.92107810, p-value = 0.16573786
bit place 6 if bit 5 = 1:
rf = 0.49599534, chi^2 =  0.04342085, p-value = 0.83493485
bit place 7 if bit 6 = 0:
rf = 0.49565925, chi^2 =  1.37346188, p-value = 0.24121797
bit place 7 if bit 6 = 1:
rf = 0.49609783, chi^2 =  0.39265145, p-value = 0.53090897
bit place 8 if bit 7 = 0:
rf = 0.49613126, chi^2 =  0.59151920, p-value = 0.44183225
bit place 8 if bit 7 = 1:
rf = 0.49566821, chi^2 =  1.26800334, p-value = 0.26014159
bit place 9 if bit 8 = 0:
rf = 0.49591823, chi^2 =  0.01146051, p-value = 0.91474634
bit place 9 if bit 8 = 1:
rf = 0.49618671, chi^2 =  0.97815988, p-value = 0.32265352
bit place 10 if bit 9 = 0:
rf = 0.49595439, chi^2 =  0.00173650, p-value = 0.96676068
bit place 10 if bit 9 = 1:
rf = 0.49574376, chi^2 =  0.66920714, p-value = 0.41332817
```

6 AIS31 evaluation tests kurz bei +85°C

```
************************************************************************
*                                                                      *
*                        AIS31 evaluation tests                        *
*                                                                      *
************************************************************************


date, time:     06/13/2019,  18:28:14
tested file:    T+85.rnd
size of file:   10485760 bytes


------------------------------------------------------------------------
Introduction
------------------------------------------------------------------------

The purpose of the following tests is to evaluate the suitability
of a true (physical) random number generator for cryptographic
```

applications. In [1] an evaluation methodology for physical random number generators has been proposed by the German Federal Security Agency. In the mathematical-technical reference to [1], five tests are defined for the P2-evaluation of a physical random number generator (cf. [3] and [4]) which are implemented in the following tests 1 - 5.

Results of test 1 (test (P2.i)(vii.a) of AIS 31, cf. [3] and [4])

In this test, the relative frequency r of bit 1 ocurring in the first 100000 bits of the bit sequence is computed. Then the bit sequence passes the test if |r - 0.5| < 0.025.

test scope: first 100000 bits
number of ones: 49723
relative frequency: 0.497230
test value: 0.00277000 < 0.025

sequence passes test 1

Results of test 2 (test (P2.i)(vii.b) of AIS 31, cf. [3] and [4])

In this test, two disjoint sub-sequences TF(0) and TF(1) of bit pairs are considered where TF(i) consists of the first 100000 bit pairs of the form (i,x) ocurring in the bit sequence after the test scope of test 1. Let v(i,j) denote the relative frequency of all bit pairs of the form (i,j) in TF(i). Then the bit sequence passes the test if |v(0,1) + v(1,0) - 1| < 0.02.

number of 2-bit words looked up: 202170
relative frequency v(0,1): 0.497870
relative frequency v(1,0): 0.504960
test value: 0.00283000 < 0.02

sequence passes test 2

Results of test 3 (test (P2.i)(vii.c) of AIS 31, cf. [3] and [4])

In this test, 4 disjoint sub-sequences TF(0,0),..., TF(1,1) of 3-tupels are considered where TF(i,j) consists of the first 100000 3-tupels of bits of the form (i,j,x) ocurring in the bit sequence after the test scope of test 2. For every i,j in {0,1}, let S(i,j) denote the sub-sequence of all bits k such that (i,j,k) is element of TF(i,j). Then sample S(0,j) is compared with S(1,j) for every j = 0,1. In this context, a comparison of two bit sequences g and h of equal length is performed by a computation of the test value t = (g_0 - h_0)^2 /(g_0 + h_0) + (g_1 - h_1)^2 /(g_1 + h_1) where g_i resp. h_i is the number of bit i occurring in sequence g resp. h. Let t_j be the test value for the comparison of S(0,j) with S(1,j) Then the bit sequence passes the test if t_j < 15,13 for j = 0,1.

number of 3-bit words looked up: 405180
test value t_1: 0.233297 <= 15.13
test value t_2: 0.018001 <= 15.13

sequence passes test 3

Results of test 4 (test (P2.i)(vii.d) of AIS 31, cf. [3] and [4])

In this test, 8 disjoint sub-sequences TF(0,0,0),..., TF(1,1,1) of 4-tupels are considered where TF(i,j,k) consists of the first 100000 4-tupels of bits of the form (i,j,k,x) ocurring in the bit sequence after the test scope of test 3. For every i,j in {0,1}, let S(i,j,k) denote the sub-sequence of all bits b such that (i,j,k,b) is an element of TF(i,j,k). Then sample S(0,j,k) is compared with S(1,j,k) for every j,k of {0,1}. In this context, a comparison of two bit

sequences g and h of equal length is performed by a computation of the test value t = (g_0 - h_0)^2 /(g_0 + h_0) + (g_1 - h_1)^2 /(g_1 + h_1) where g_i resp. h_i is the number of bit i occurring in sequence g resp. h. Let t_jk be the test value for the comparison of S(0,j,k) with S(1,j,k). Then the bit sequence passes the test if t_jk < 15,13 for all j,k of {0,1}.

number of 4-bit words looked up: 820932
test value t_00: 0.968034 <= 15.13
test value t_01: 0.432201 <= 15.13
test value t_10: 2.048089 <= 15.13
test value t_11: 1.240112 <= 15.13

sequence passes test 4

Results of test 5 (test (P2.i)(vii.e) of AIS 31, cf. [3] and [4])

In this test, the Coron test with the parameters L = 8, Q = 2560, and K = 256000 is performed (cf. [2]). For the first Q+K 8-bit-words after the test scope of test 4, the test value f of the Coron test is computed. The bit sequence passes the test if f > 7.976.

8-bit words looked up: 2560 + 256000 bytes
f-value: 7.99544254
7.99544254 > 7.976

sequence passes test 5

References

---

[1] AIS 31: Functionality Classes and Evaluation Methodology for Physical Random Number Generators. Version 1 (25.09.2001), (mandatory if a German IT security certificate is applied for; English translation).
available at www.bsi.bund.de/zertifiz/zert/interpr/ais31e.pdf

[2] J.- S. Coron: On the Security of Random Sources. In: Public Key Cryptography - PKC 99. Lecture Notes in Computer Science, Vol. 1560, 29-42, Springer-Verlag, 2002.

[3] W. Killmann and W. Schindler: A Proposal for: Functionality Classes and Evaluation Methodology for True (Physical) Random Number Generators. Version 3.1 (25.09.2001), mathematical-technical reference of [1] (English Translation);
available at www.bsi.bund.de/zertifiz/zert/interpr/trngk31e.pdf

[4] W. Schindler and W. Killmann: Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications. In: Cryptographic Hardware and Empedded Systems - CHES 2002. Lecture Notes in Computer Science, Vol. 2523, 431-449, Springer-Verlag, 2002.

7 AIS31 evaluation tests lang bei +85°C

```
################################################################################
#                                                                              #
#                            Results of RawTest                                #
#                                                                              #
################################################################################


date, time:     06/13/2019,  18:28:29
tested file:    T+85.rnd
size of file:   10485760 bytes


********************************************************************************
*                                                                              *
*                     Results of the frequency test                            *
*                                                                              *
********************************************************************************


test scope:      first 10485760 bytes
relative frequency of bit 1:  0.49610877

block length L =  2:  chi^2 =      1.3973,  p-value = 0.70616620
block length L =  3:  chi^2 =      8.3834,  p-value = 0.29999962
block length L =  4:  chi^2 =     18.4087,  p-value = 0.24178716
block length L =  5:  chi^2 =     32.6912,  p-value = 0.38384070
block length L =  6:  chi^2 =     61.5262,  p-value = 0.52901044
block length L =  7:  chi^2 =    132.2163,  p-value = 0.35769421
block length L =  8:  chi^2 =    277.7506,  p-value = 0.15667040
block length L =  9:  chi^2 =    533.9357,  p-value = 0.23338010
block length L = 10:  chi^2 =    937.5990,  p-value = 0.97310021


********************************************************************************
*                                                                              *
*                       Results of the serial test                             *
*                                                                              *
********************************************************************************


test scope:      first 10000000 bytes
relative frequency of bit 1:  0.49609514

block length L =  2:  chi^2 =      3.2431,  p-value = 0.19759399
block length L =  3:  chi^2 =      5.7023,  p-value = 0.22250958
block length L =  4:  chi^2 =      9.6436,  p-value = 0.29093582
block length L =  5:  chi^2 =     16.6348,  p-value = 0.40959943
block length L =  6:  chi^2 =     47.7131,  p-value = 0.03654807
block length L =  7:  chi^2 =     82.8930,  p-value = 0.05628095
block length L =  8:  chi^2 =    135.6280,  p-value = 0.30534887
block length L =  9:  chi^2 =    266.2432,  p-value = 0.31698067
block length L = 10:  chi^2 =    515.8624,  p-value = 0.44384840


********************************************************************************
*                                                                              *
*                  Results of the modular monobit test                         *
*                                                                              *
********************************************************************************


test scope:      first 10485760 bytes
relative frequency of bit 1:  0.49610877

modular monobit test for block length L = 3:
bit  0:  rf = 0.49607500, chi^2 =  0.12757650, p-value = 0.72095816
bit  1:  rf = 0.49624659, chi^2 =  2.12454223, p-value = 0.14495608
bit  2:  rf = 0.49600472, chi^2 =  1.21089197, p-value = 0.27115554

modular monobit test for block length L = 4:
bit  0:  rf = 0.49640293, chi^2 =  7.25915262, p-value = 0.00705406
```

```
bit  1:  rf = 0.49611430, chi^2 =  0.00256668, p-value = 0.95959450
bit  2:  rf = 0.49591198, chi^2 =  3.24881757, p-value = 0.07147500
bit  3:  rf = 0.49600587, chi^2 =  0.88829919, p-value = 0.34593863

modular monobit test for block length L = 5:
bit  0:  rf = 0.49604023, chi^2 =  0.31532767, p-value = 0.57442917
bit  1:  rf = 0.49610680, chi^2 =  0.00025965, p-value = 0.98714363
bit  2:  rf = 0.49610579, chi^2 =  0.00059608, p-value = 0.98052174
bit  3:  rf = 0.49610889, chi^2 =  0.00000095, p-value = 0.99922079
bit  4:  rf = 0.49618214, chi^2 =  0.36131210, p-value = 0.54777843

modular monobit test for block length L = 6:
bit  0:  rf = 0.49615010, chi^2 =  0.09553244, p-value = 0.75725821
bit  1:  rf = 0.49616390, chi^2 =  0.17000714, p-value = 0.68010546
bit  2:  rf = 0.49599303, chi^2 =  0.74919497, p-value = 0.38673123
bit  3:  rf = 0.49599990, chi^2 =  0.66293784, p-value = 0.41552469
bit  4:  rf = 0.49632927, chi^2 =  2.71923902, p-value = 0.09914527
bit  5:  rf = 0.49601642, chi^2 =  0.47699425, p-value = 0.48978696

modular monobit test for block length L = 7:
bit  0:  rf = 0.49585350, chi^2 =  3.12373718, p-value = 0.07715963
bit  1:  rf = 0.49619722, chi^2 =  0.37501219, p-value = 0.54028479
bit  2:  rf = 0.49616451, chi^2 =  0.14891927, p-value = 0.69957029
bit  3:  rf = 0.49623644, chi^2 =  0.78133125, p-value = 0.37673431
bit  4:  rf = 0.49611861, chi^2 =  0.00464207, p-value = 0.94567995
bit  5:  rf = 0.49603633, chi^2 =  0.25154064, p-value = 0.61599235
bit  6:  rf = 0.49615483, chi^2 =  0.10168475, p-value = 0.74981716

modular monobit test for block length L = 8:
bit  0:  rf = 0.49656305, chi^2 =  8.65642801, p-value = 0.00325910
bit  1:  rf = 0.49597692, chi^2 =  0.72914963, p-value = 0.39315896
bit  2:  rf = 0.49588337, chi^2 =  2.13106941, p-value = 0.14434002
bit  3:  rf = 0.49615870, chi^2 =  0.10454897, p-value = 0.74643751
bit  4:  rf = 0.49624281, chi^2 =  0.75361248, p-value = 0.38533490
bit  5:  rf = 0.49625168, chi^2 =  0.85664301, p-value = 0.35467983
bit  6:  rf = 0.49594059, chi^2 =  1.18641686, p-value = 0.27605351
bit  7:  rf = 0.49585304, chi^2 =  2.74310218, p-value = 0.09767498

modular monobit test for block length L = 9:
bit  0:  rf = 0.49606740, chi^2 =  0.06381795, p-value = 0.80056021
bit  1:  rf = 0.49633551, chi^2 =  1.91688863, p-value = 0.16620006
bit  2:  rf = 0.49585701, chi^2 =  2.36331699, p-value = 0.12421782
bit  3:  rf = 0.49619443, chi^2 =  0.27356816, p-value = 0.60094820
bit  4:  rf = 0.49641255, chi^2 =  3.44062479, p-value = 0.06361163
bit  5:  rf = 0.49616600, chi^2 =  0.12210216, p-value = 0.72676562
bit  6:  rf = 0.49596322, chi^2 =  0.78986170, p-value = 0.37414195
bit  7:  rf = 0.49599165, chi^2 =  0.51141863, p-value = 0.47452539
bit  8:  rf = 0.49599122, chi^2 =  0.51517348, p-value = 0.47290783

modular monobit test for block length L = 10:
bit  0:  rf = 0.49593711, chi^2 =  0.98882942, p-value = 0.32002864
bit  1:  rf = 0.49607384, chi^2 =  0.04093847, p-value = 0.83965673
bit  2:  rf = 0.49637580, chi^2 =  2.39272304, p-value = 0.12190113
bit  3:  rf = 0.49625254, chi^2 =  0.69357114, p-value = 0.40495235
bit  4:  rf = 0.49636936, chi^2 =  2.27875015, p-value = 0.13115753
bit  5:  rf = 0.49614334, chi^2 =  0.04010443, p-value = 0.84127653
bit  6:  rf = 0.49613976, chi^2 =  0.03223614, p-value = 0.85751036
bit  7:  rf = 0.49583578, chi^2 =  2.50073320, p-value = 0.11379331
bit  8:  rf = 0.49596524, chi^2 =  0.69127264, p-value = 0.40573185
bit  9:  rf = 0.49599493, chi^2 =  0.43491375, p-value = 0.50958764


**************************************************************************
*                                                                        *
*                 Results of the autocorrelation test                    *
*                                                                        *
**************************************************************************


test scope:     first 10000000 bytes
relative frequency of bit 1:  0.49609514

bit shift d =  1:  chi^2 =  3.24267914,  p-value = 0.07174323
bit shift d =  2:  chi^2 =  1.94917213,  p-value = 0.16267609
bit shift d =  3:  chi^2 =  0.58624775,  p-value = 0.44387377
bit shift d =  4:  chi^2 =  0.02357593,  p-value = 0.87796887
bit shift d =  5:  chi^2 =  6.38091653,  p-value = 0.01153538
```

```
bit shift d =  6:  chi^2 =  0.36729392,  p-value = 0.54448302
bit shift d =  7:  chi^2 =  0.44158813,  p-value = 0.50635693
bit shift d =  8:  chi^2 =  1.42881057,  p-value = 0.23195865
bit shift d =  9:  chi^2 =  0.00092246,  p-value = 0.97577031
bit shift d = 10:  chi^2 =  0.01059510,  p-value = 0.91801654


*********************************************************************
*                                                                   *
*                   Results of the dependency test                  *
*                                                                   *
*********************************************************************


test scope:     first 10485760 bytes
relative frequency of bit 1:  0.49610877

dependency test for block length L = 3:

bit place 1 if bit 0 = 0:
rf = 0.49642450, chi^2 =  5.61896074, p-value = 0.01776718
bit place 1 if bit 0 = 1:
rf = 0.49606582, chi^2 =  0.10234710, p-value = 0.74903100
bit place 2 if bit 1 = 0:
rf = 0.49609803, chi^2 =  0.00649853, p-value = 0.93574935
bit place 2 if bit 1 = 1:
rf = 0.49591004, chi^2 =  2.19216199, p-value = 0.13871449
bit place 3 if bit 2 = 0:
rf = 0.49607216, chi^2 =  0.07556523, p-value = 0.78339974
bit place 3 if bit 2 = 1:
rf = 0.49607785, chi^2 =  0.05305235, p-value = 0.81783461

dependency test for block length L = 4:

bit place 1 if bit 0 = 0:
rf = 0.49617297, chi^2 =  0.17413348, p-value = 0.67646408
bit place 1 if bit 0 = 1:
rf = 0.49605483, chi^2 =  0.12116792, p-value = 0.72777122
bit place 2 if bit 1 = 0:
rf = 0.49592032, chi^2 =  1.50122715, p-value = 0.22048264
bit place 2 if bit 1 = 1:
rf = 0.49590356, chi^2 =  1.75270164, p-value = 0.18553746
bit place 3 if bit 2 = 0:
rf = 0.49606607, chi^2 =  0.07710367, p-value = 0.78126148
bit place 3 if bit 2 = 1:
rf = 0.49594463, chi^2 =  1.12091114, p-value = 0.28972235
bit place 4 if bit 3 = 0:
rf = 0.49663358, chi^2 = 11.64496028, p-value = 0.00064377
bit place 4 if bit 3 = 1:
rf = 0.49616852, chi^2 =  0.14856921, p-value = 0.69990644

dependency test for block length L = 5:

bit place 1 if bit 0 = 0:
rf = 0.49632959, chi^2 =  1.64915711, p-value = 0.19907369
bit place 1 if bit 0 = 1:
rf = 0.49588040, chi^2 =  1.73616021, p-value = 0.18762609
bit place 2 if bit 1 = 0:
rf = 0.49601020, chi^2 =  0.32860092, p-value = 0.56648408
bit place 2 if bit 1 = 1:
rf = 0.49620294, chi^2 =  0.29528269, p-value = 0.58685498
bit place 3 if bit 2 = 0:
rf = 0.49632390, chi^2 =  1.56516992, p-value = 0.21090985
bit place 3 if bit 2 = 1:
rf = 0.49589056, chi^2 =  1.58538083, p-value = 0.20798733
bit place 4 if bit 3 = 0:
rf = 0.49620027, chi^2 =  0.28312396, p-value = 0.59466094
bit place 4 if bit 3 = 1:
rf = 0.49616367, chi^2 =  0.10036216, p-value = 0.75139546
bit place 5 if bit 4 = 0:
rf = 0.49612720, chi^2 =  0.01147944, p-value = 0.91467621
bit place 5 if bit 4 = 1:
rf = 0.49595186, chi^2 =  0.81993070, p-value = 0.36520043

dependency test for block length L = 6:

bit place 1 if bit 0 = 0:
```

```
rf = 0.49628283, chi^2 =  0.85370487, p-value = 0.35550636
bit place 1 if bit 0 = 1:
rf = 0.49604306, chi^2 =  0.11979955, p-value = 0.72925200
bit place 2 if bit 1 = 0:
rf = 0.49609754, chi^2 =  0.00355651, p-value = 0.95244515
bit place 2 if bit 1 = 1:
rf = 0.49588684, chi^2 =  1.36678832, p-value = 0.24236446
bit place 3 if bit 2 = 0:
rf = 0.49597717, chi^2 =  0.48819179, p-value = 0.48473502
bit place 3 if bit 2 = 1:
rf = 0.49602306, chi^2 =  0.20376427, p-value = 0.65169944
bit place 4 if bit 3 = 0:
rf = 0.49656613, chi^2 =  5.89628824, p-value = 0.01517283
bit place 4 if bit 3 = 1:
rf = 0.49608852, chi^2 =  0.01137962, p-value = 0.91504658
bit place 5 if bit 4 = 0:
rf = 0.49609853, chi^2 =  0.00295585, p-value = 0.95664218
bit place 5 if bit 4 = 1:
rf = 0.49593317, chi^2 =  0.85596457, p-value = 0.35487045
bit place 6 if bit 5 = 0:
rf = 0.49616715, chi^2 =  0.09607765, p-value = 0.75658838
bit place 6 if bit 5 = 1:
rf = 0.49613270, chi^2 =  0.01588491, p-value = 0.89970393

dependency test for block length L = 7:

bit place 1 if bit 0 = 0:
rf = 0.49617962, chi^2 =  0.12132758, p-value = 0.72759905
bit place 1 if bit 0 = 1:
rf = 0.49621519, chi^2 =  0.26919316, p-value = 0.60387352
bit place 2 if bit 1 = 0:
rf = 0.49622480, chi^2 =  0.32516035, p-value = 0.56852284
bit place 2 if bit 1 = 1:
rf = 0.49610320, chi^2 =  0.00073777, p-value = 0.97833053
bit place 3 if bit 2 = 0:
rf = 0.49627382, chi^2 =  0.65798968, p-value = 0.41727056
bit place 3 if bit 2 = 1:
rf = 0.49619856, chi^2 =  0.19174083, p-value = 0.66147167
bit place 4 if bit 3 = 0:
rf = 0.49615378, chi^2 =  0.04891891, p-value = 0.82495524
bit place 4 if bit 3 = 1:
rf = 0.49608283, chi^2 =  0.01601278, p-value = 0.89930321
bit place 5 if bit 4 = 0:
rf = 0.49622630, chi^2 =  0.33367607, p-value = 0.56350246
bit place 5 if bit 4 = 1:
rf = 0.49584330, chi^2 =  1.67602411, p-value = 0.19545359
bit place 6 if bit 5 = 0:
rf = 0.49621036, chi^2 =  0.24933725, p-value = 0.61754213
bit place 6 if bit 5 = 1:
rf = 0.49609832, chi^2 =  0.00259704, p-value = 0.95935648
bit place 7 if bit 6 = 0:
rf = 0.49611888, chi^2 =  0.00246675, p-value = 0.96038826
bit place 7 if bit 6 = 1:
rf = 0.49558393, chi^2 =  6.55167978, p-value = 0.01047852

dependency test for block length L = 8:

bit place 1 if bit 0 = 0:
rf = 0.49596594, chi^2 =  0.43082420, p-value = 0.51158480
bit place 1 if bit 0 = 1:
rf = 0.49598797, chi^2 =  0.30394810, p-value = 0.58141784
bit place 2 if bit 1 = 0:
rf = 0.49593770, chi^2 =  0.61868194, p-value = 0.43153751
bit place 2 if bit 1 = 1:
rf = 0.49582806, chi^2 =  1.63936037, p-value = 0.20041325
bit place 3 if bit 2 = 0:
rf = 0.49611505, chi^2 =  0.00083507, p-value = 0.97694626
bit place 3 if bit 2 = 1:
rf = 0.49620316, chi^2 =  0.18530018, p-value = 0.66685737
bit place 4 if bit 3 = 0:
rf = 0.49635199, chi^2 =  1.25021894, p-value = 0.26351067
bit place 4 if bit 3 = 1:
rf = 0.49613184, chi^2 =  0.01107485, p-value = 0.91618765
bit place 5 if bit 4 = 0:
rf = 0.49637988, chi^2 =  1.55304189, p-value = 0.21268694
bit place 5 if bit 4 = 1:
rf = 0.49612164, chi^2 =  0.00344514, p-value = 0.95319479
bit place 6 if bit 5 = 0:
```

```
rf = 0.49590292, chi^2 =  0.89532769, p-value = 0.34403763
bit place 6 if bit 5 = 1:
rf = 0.49597892, chi^2 =  0.35097851, p-value = 0.55355974
bit place 7 if bit 6 = 0:
rf = 0.49601708, chi^2 =  0.17774896, p-value = 0.67331493
bit place 7 if bit 6 = 1:
rf = 0.49568622, chi^2 =  3.71422900, p-value = 0.05395054
bit place 8 if bit 7 = 0:
rf = 0.49691489, chi^2 = 13.74185293, p-value = 0.00020973
bit place 8 if bit 7 = 1:
rf = 0.49620523, chi^2 =  0.19352828, p-value = 0.65999615

dependency test for block length L = 9:

bit place 1 if bit 0 = 0:
rf = 0.49669107, chi^2 =  6.37095852, p-value = 0.01160029
bit place 1 if bit 0 = 1:
rf = 0.49597420, chi^2 =  0.33492428, p-value = 0.56277378
bit place 2 if bit 1 = 0:
rf = 0.49590424, chi^2 =  0.78555309, p-value = 0.37544817
bit place 2 if bit 1 = 1:
rf = 0.49580918, chi^2 =  1.66100033, p-value = 0.19746832
bit place 3 if bit 2 = 0:
rf = 0.49617894, chi^2 =  0.09253936, p-value = 0.76097338
bit place 3 if bit 2 = 1:
rf = 0.49621029, chi^2 =  0.19053045, p-value = 0.66247549
bit place 4 if bit 3 = 0:
rf = 0.49636559, chi^2 =  1.23892285, p-value = 0.26567875
bit place 4 if bit 3 = 1:
rf = 0.49646011, chi^2 =  2.28376152, p-value = 0.13073446
bit place 5 if bit 4 = 0:
rf = 0.49645925, chi^2 =  2.30635199, p-value = 0.12884613
bit place 5 if bit 4 = 1:
rf = 0.49586862, chi^2 =  1.06748072, p-value = 0.30151518
bit place 6 if bit 5 = 0:
rf = 0.49593235, chi^2 =  0.58471244, p-value = 0.44447110
bit place 6 if bit 5 = 1:
rf = 0.49599447, chi^2 =  0.24170489, p-value = 0.62297746
bit place 7 if bit 6 = 0:
rf = 0.49621676, chi^2 =  0.21917795, p-value = 0.63966699
bit place 7 if bit 6 = 1:
rf = 0.49576277, chi^2 =  2.21381713, p-value = 0.13677986
bit place 8 if bit 7 = 0:
rf = 0.49593077, chi^2 =  0.59538658, p-value = 0.44034369
bit place 8 if bit 7 = 1:
rf = 0.49605254, chi^2 =  0.05846648, p-value = 0.80893636
bit place 9 if bit 8 = 0:
rf = 0.49610512, chi^2 =  0.00025083, p-value = 0.98736398
bit place 9 if bit 8 = 1:
rf = 0.49602896, chi^2 =  0.11779053, p-value = 0.73144331

dependency test for block length L = 10:

bit place 1 if bit 0 = 0:
rf = 0.49633193, chi^2 =  0.84237751, p-value = 0.35871769
bit place 1 if bit 0 = 1:
rf = 0.49581164, chi^2 =  1.46924601, p-value = 0.22546469
bit place 2 if bit 1 = 0:
rf = 0.49636098, chi^2 =  1.07564578, p-value = 0.29967367
bit place 2 if bit 1 = 1:
rf = 0.49639073, chi^2 =  1.32342569, p-value = 0.24997817
bit place 3 if bit 2 = 0:
rf = 0.49643028, chi^2 =  1.74695593, p-value = 0.18625987
bit place 3 if bit 2 = 1:
rf = 0.49607207, chi^2 =  0.02243166, p-value = 0.88094449
bit place 4 if bit 3 = 0:
rf = 0.49639045, chi^2 =  1.34126444, p-value = 0.24681110
bit place 4 if bit 3 = 1:
rf = 0.49634783, chi^2 =  0.95167694, p-value = 0.32929281
bit place 5 if bit 4 = 0:
rf = 0.49616594, chi^2 =  0.05522798, p-value = 0.81420382
bit place 5 if bit 4 = 1:
rf = 0.49612053, chi^2 =  0.00230523, p-value = 0.96170602
bit place 6 if bit 5 = 0:
rf = 0.49632724, chi^2 =  0.80696609, p-value = 0.36901875
bit place 6 if bit 5 = 1:
rf = 0.49594926, chi^2 =  0.42362371, p-value = 0.51513440
bit place 7 if bit 6 = 0:
```

```
rf = 0.49565925, chi^2 =  3.41657424, p-value = 0.06454482
bit place 7 if bit 6 = 1:
rf = 0.49601518, chi^2 =  0.14582400, p-value = 0.70255847
bit place 8 if bit 7 = 0:
rf = 0.49621764, chi^2 =  0.20051248, p-value = 0.65430750
bit place 8 if bit 7 = 1:
rf = 0.49570873, chi^2 =  2.66273421, p-value = 0.10272402
bit place 9 if bit 8 = 0:
rf = 0.49601019, chi^2 =  0.16435927, p-value = 0.68517434
bit place 9 if bit 8 = 1:
rf = 0.49597929, chi^2 =  0.27902507, p-value = 0.59734093
bit place 10 if bit 9 = 0:
rf = 0.49608848, chi^2 =  0.00695978, p-value = 0.93351338
bit place 10 if bit 9 = 1:
rf = 0.49578317, chi^2 =  1.76453222, p-value = 0.18406021
```