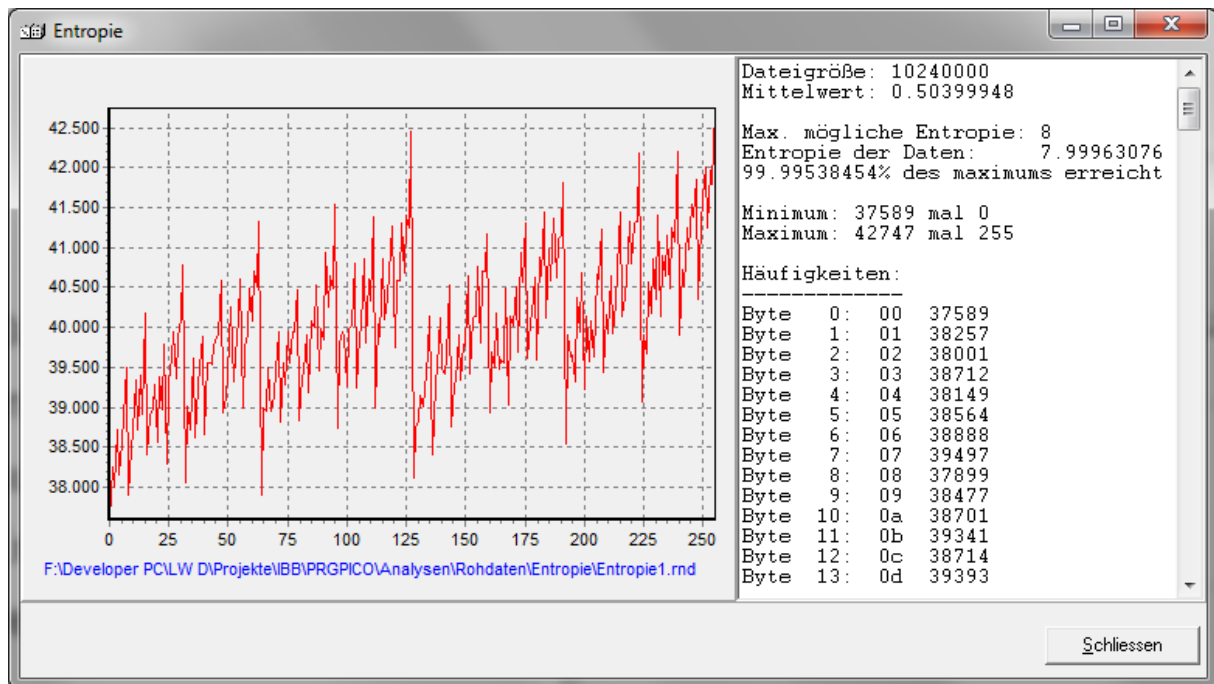


## Rohdaten-Analyse von diversen PRG600-Modulen

Das folgende Dokument analysiert Zufalls-Rohdaten des PRG600. Hierzu wurde die Firmware modifiziert, so dass die digitalisierten Rauschsignale direkt (ohne Nachbearbeitung nach Schema) ausgegeben werden. Es wurden jeweils Dateien von 10Mbyte generiert. In der Analyse werden die Entropie, die Gleichverteilung der logischen Bits (0,1), die Häufigkeit der 256 möglichen Bytes und relevante Analysen nach AIS31 aufgelistet.

### Modul 1:



Häufigkeitsanalyse: die Struktur ist nicht durch deterministische Anteile, sondern ausschließlich durch die Schiefe der 0/1-Anteile bedingt (1-Bits > 0-Bits).

Mittelwert: 0.50399948

Entropie der Daten: 7.99963076 (nach Shannon)

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

```
date, time:    08/07/2014, 11:54:43
tested file:   Entropie1.rnd
size of file: 10240000 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 occurring 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: 50284  
 relative frequency: 0.502840  
 test value: 0.00284000 < 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  $(i,x)$  occurring 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: 201575  
 relative frequency  $v(0,1)$ : 0.503020  
 relative frequency  $v(1,0)$ : 0.495090  
 test value: 0.00189000 < 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  $TF(0,0), \dots, TF(1,1)$  of 3-tupels are considered where  $TF(i,j)$  consists of the first 100000 3-tupels of bits of the form  $(i,j,x)$  occurring 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: 404673  
 test value  $t_1$ : 0.278494 <= 15.13  
 test value  $t_2$ : 1.003565 <= 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  $TF(0,0,0), \dots, TF(1,1,1)$  of 4-tupels are considered where  $TF(i,j,k)$  consists of the first 100000 4-tupels of bits of the form  $(i,j,k,x)$  occurring 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: 821561  
 test value  $t_{00}$ : 0.040505  $\leq$  15.13  
 test value  $t_{01}$ : 0.000180  $\leq$  15.13  
 test value  $t_{10}$ : 0.100830  $\leq$  15.13  
 test value  $t_{11}$ : 3.477892  $\leq$  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  $f > 7.976$ .

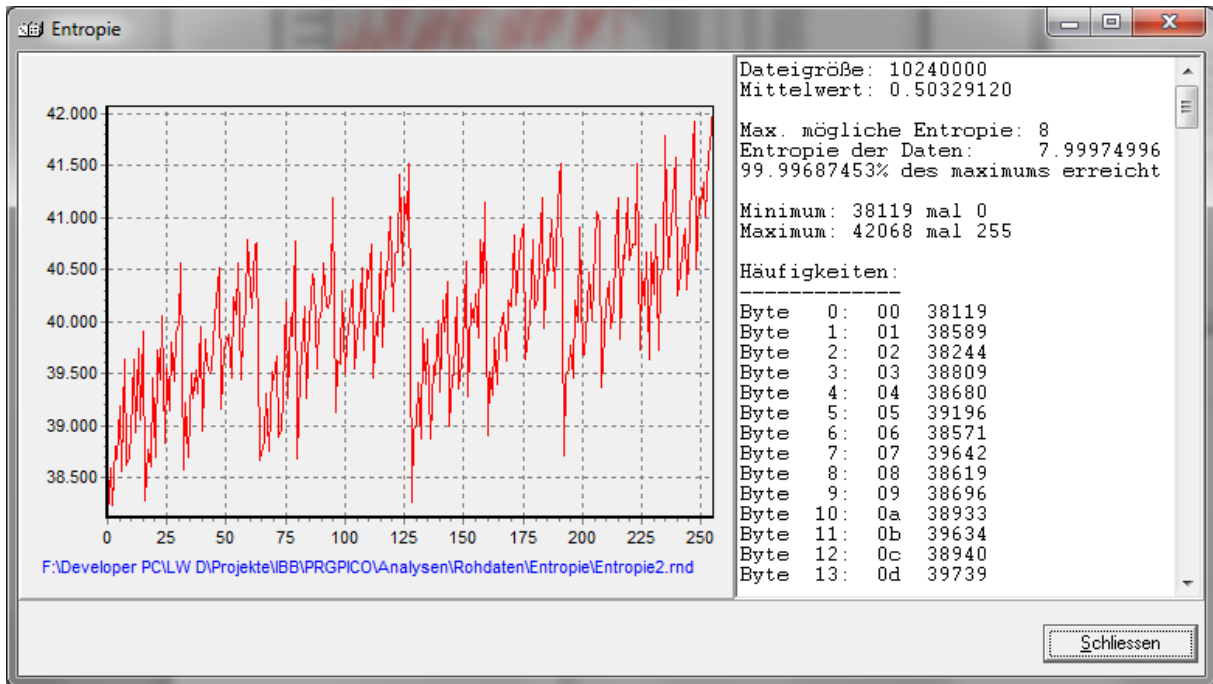
8-bit words looked up: 2560 + 256000 bytes  
 f-value: 7.99930378  
 7.99930378  $>$  7.976

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](http://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](http://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 Embedded Systems - CHES 2002. Lecture Notes in Computer Science, Vol. 2523, 431-449, Springer-Verlag, 2002.

**Modul 2:**



Mittelwert: 0.50329120  
Entropie der Daten: 7.99974996

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

```
date, time:    08/07/2014, 11:59:45
tested file:   Entropie2.rnd
size of file: 10240000 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 occurring 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: 50364  
 relative frequency: 0.503640  
 test value: 0.00364000 < 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) occurring 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: 202348  
 relative frequency  $v(0,1)$ : 0.504320  
 relative frequency  $v(1,0)$ : 0.496580  
 test value: 0.00090000 < 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) occurring 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: 407139  
 test value  $t_1$ : 6.844948  $\leq$  15.13  
 test value  $t_2$ : 1.104539  $\leq$  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) occurring 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: 815636  
test value  $t_{00}$ : 0.002000  $\leq$  15.13  
test value  $t_{01}$ : 0.348497  $\leq$  15.13  
test value  $t_{10}$ : 0.176734  $\leq$  15.13  
test value  $t_{11}$ : 0.011520  $\leq$  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  $f > 7.976$ .

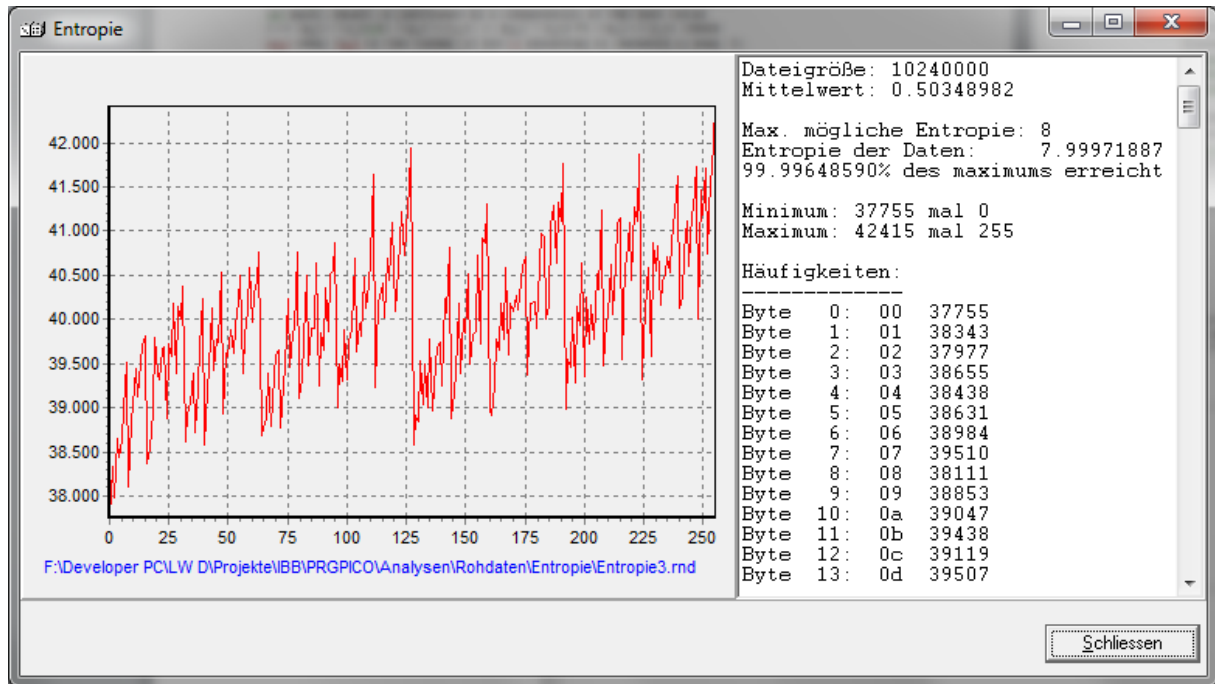
8-bit words looked up: 2560 + 256000 bytes  
f-value: 8.00262303  
8.00262303  $>$  7.976

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](http://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](http://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 Embedded Systems - CHES 2002. Lecture Notes in Computer Science, Vol. 2523, 431-449, Springer-Verlag, 2002.

**Modul 3:**



Mittelwert: 0.50348982

Entropie der Daten: 7.99971887

```

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

```

date, time:    08/07/2014, 12:02:34
tested file:   Entropie3.rnd
size of file: 10240000 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 occurring 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: 50524
relative frequency: 0.505240
test value: 0.00524000 < 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) occurring 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: 201450
relative frequency v(0,1): 0.503430
relative frequency v(1,0): 0.496660
test value: 0.00009000 < 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) occurring 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: 404748
test value t_1: 0.480524 <= 15.13
test value t_2: 0.353797 <= 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) occurring 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: 817351  
test value t\_00: 1.717109 <= 15.13  
test value t\_01: 1.601861 <= 15.13  
test value t\_10: 11.012114 <= 15.13  
test value t\_11: 0.220506 <= 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  $f > 7.976$ .

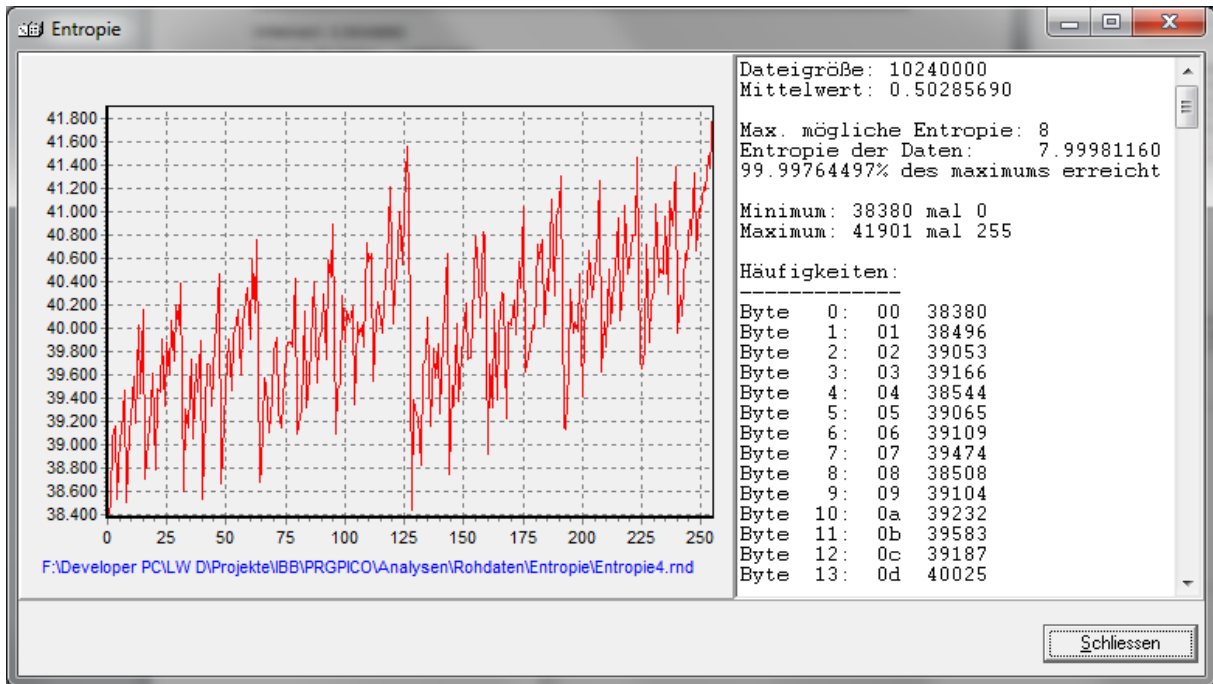
8-bit words looked up: 2560 + 256000 bytes  
f-value: 7.99842872  
7.99842872 > 7.976

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](http://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](http://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 Embedded Systems - CHES 2002. Lecture Notes in Computer Science, Vol. 2523, 431-449, Springer-Verlag, 2002.

**Modul 4:**



Mittelwert: 0.50285690

Entropie der Daten: 7.99981160

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

```
date, time:    08/07/2014, 12:05:14
tested file:   Entropie4.rnd
size of file: 10240000 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 occurring 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: 50316
relative frequency: 0.503160
test value: 0.00316000 < 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) occurring 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: 202079
relative frequency v(0,1): 0.502830
relative frequency v(1,0): 0.495460
test value: 0.00171000 < 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) occurring 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: 403514
test value t_1: 0.648009 <= 15.13
test value t_2: 0.662487 <= 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) occurring 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: 812371  
test value t\_00: 0.010580 <= 15.13  
test value t\_01: 0.865298 <= 15.13  
test value t\_10: 3.544893 <= 15.13  
test value t\_11: 3.073362 <= 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  $f > 7.976$ .

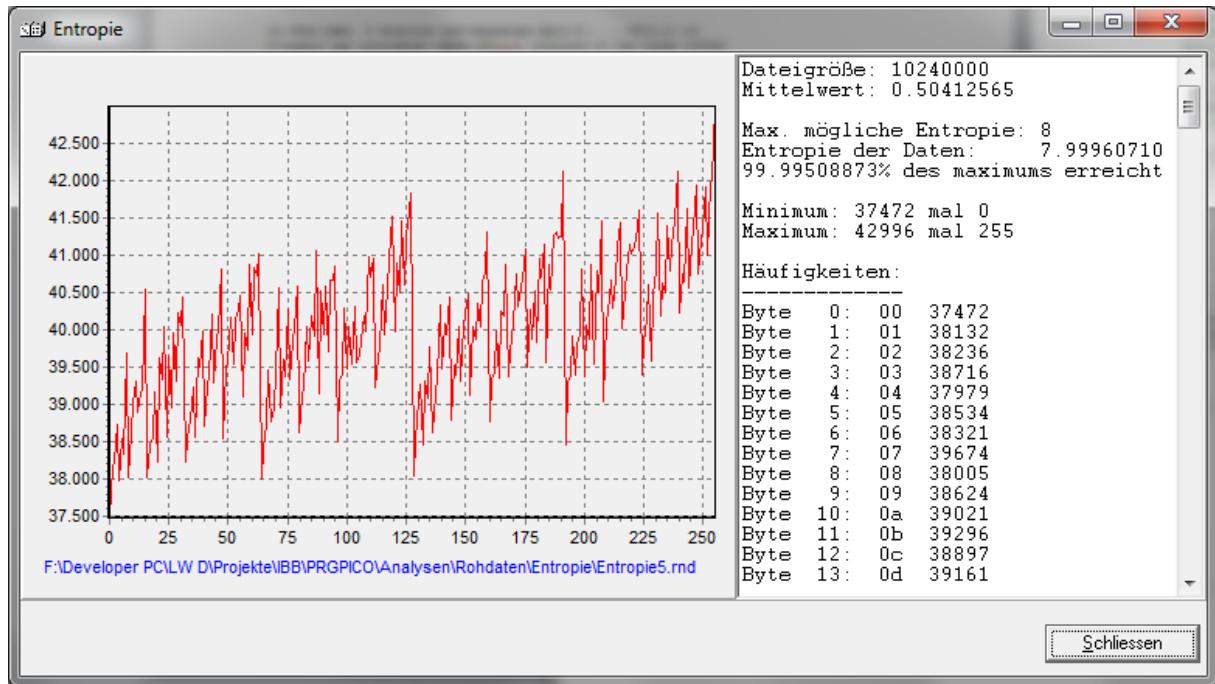
8-bit words looked up: 2560 + 256000 bytes  
f-value: 7.99652686  
7.99652686 > 7.976

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](http://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](http://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 Embedded Systems - CHES 2002. Lecture Notes in Computer Science, Vol. 2523, 431-449, Springer-Verlag, 2002.

**Modul 5:**



Mittelwert: 0.50412565

Entropie der Daten: 7.99960710

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

```
date, time:    08/07/2014, 12:07:42
tested file:   Entropie5.rnd
size of file: 10240000 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 occurring 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: 50622
relative frequency: 0.506220
test value: 0.00622000 < 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) occurring 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: 201935
relative frequency v(0,1): 0.507000
relative frequency v(1,0): 0.498870
test value: 0.00587000 < 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) occurring 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: 406953
test value t_1: 0.426344 <= 15.13
test value t_2: 1.717125 <= 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) occurring 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: 822776  
test value t\_00: 2.125764 <= 15.13  
test value t\_01: 1.152009 <= 15.13  
test value t\_10: 13.778792 <= 15.13  
test value t\_11: 0.677162 <= 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: 7.99665644  
7.99665644 > 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](http://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](http://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 Embedded Systems - CHES 2002. Lecture Notes in Computer Science, Vol. 2523, 431-449, Springer-Verlag, 2002.