

Test drei verschiedener PRG420-Geräte (M1, M2, M3)

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

date, time: 12/17/2017, 13:55:58  
tested file: m1+20.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: 49453  
relative frequency: 0.494530  
test value: 0.00547000 < 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: 202628  
relative frequency  $v(0,1)$ : 0.495720  
relative frequency  $v(1,0)$ : 0.505570

test value: 0.00129000 < 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: 409265

test value  $t_1$ : 3.698654  $\leq$  15.13

test value  $t_2$ : 0.584882  $\leq$  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  $TF(0,0,0), \dots, TF(1,1,1)$  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: 824735

test value  $t_{00}$ : 2.231332  $\leq$  15.13

test value  $t_{01}$ : 0.462132  $\leq$  15.13

test value  $t_{10}$ : 0.288042  $\leq$  15.13

test value  $t_{11}$ : 7.057227  $\leq$  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: 8.00017853  
8.00017853 > 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.

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

```
date, time:    12/17/2017,  13:56:22
tested file:   m2+20.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:  49323
relative frequency:  0.493230
test value:  0.00677000 < 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: 202443
relative frequency v(0,1):  0.492330
relative frequency v(1,0):  0.505760
test value:  0.00191000 < 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: 411950  
test value  $t_1$ : 0.089807  $\leq$  15.13  
test value  $t_2$ : 0.816266  $\leq$  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  $TF(0,0,0), \dots, TF(1,1,1)$  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: 840914  
test value  $t_{00}$ : 0.792210  $\leq$  15.13  
test value  $t_{01}$ : 0.012505  $\leq$  15.13  
test value  $t_{10}$ : 1.191080  $\leq$  15.13  
test value  $t_{11}$ : 0.255420  $\leq$  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: 7.99765611

7.99765611 > 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.

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

```
date, time:    12/17/2017,  13:56:43
tested file:   m3+20.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:  49931
relative frequency:  0.499310
test value:  0.00069000 < 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: 200911
relative frequency v(0,1):  0.498290
relative frequency v(1,0):  0.502500
test value:  0.00079000 < 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: 402351  
test value  $t_1$ : 0.144503  $\leq$  15.13  
test value  $t_2$ : 0.392011  $\leq$  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  $TF(0,0,0), \dots, TF(1,1,1)$  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: 810767  
test value  $t_{00}$ : 0.619521  $\leq$  15.13  
test value  $t_{01}$ : 0.250885  $\leq$  15.13  
test value  $t_{10}$ : 0.317528  $\leq$  15.13  
test value  $t_{11}$ : 1.290324  $\leq$  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: 8.00059430

8.00059430 > 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.