

## Hochwertiger physikalischer Zufallsgenerator für kryptographische Applikationen

Für die Erzeugung unvorhersagbarer Parameter werden in hochwertigen kryptographischen Applikationen physikalische Zufallsgeneratoren (TRNG) eingesetzt. Die meisten bekannten physikalischen Zufallsgeneratoren sind nur mit hohem Aufwand stabil in ihren Parametern einzustellen. Spannungs- und Temperaturschwankungen sowie elektromagnetische Störungen beeinflussen Entropie und statistische Ergebnisse negativ, so dass oftmals nur durch Nachbearbeitung mit mathematischen Algorithmen die erforderliche statistische Qualität gewährleistet werden kann. Der patentierte und bereits in zahlreichen Applikationen implementierte physikalische Zufallsgenerator zeichnet sich vor allem durch folgende Eigenschaften aus:

- Kleine Schaltung mit Standardbauelementen
- Kontinuierlicher automatischer Abgleich der gesamten Schaltung
- Digitalisierte Zufallsrohdaten mit 6.8 MHz
- Stabile Ausgabedaten auch bei Spannungs- und Temperaturschwankungen (Spannung: 10%, Temperatur -20..+85°C)
- Sehr hohe Entropie der Rohdaten (>7,997 Bit/Byte); das entspricht einer Wahrscheinlichkeit  $p$  von Bit 1 der Rohdaten von  $0.49 \leq p \leq 0.51$
- Keine Schirmung oder spezielle Filtermaßnahmen bei der Implementierung notwendig
- Problemlos und kostengünstig in hohen Stückzahlen zu fertigen

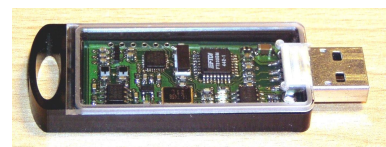
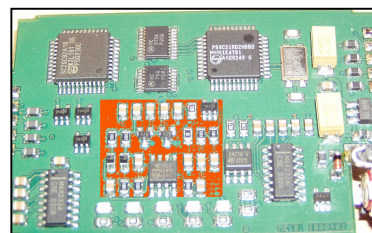
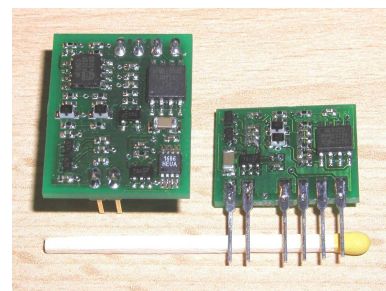
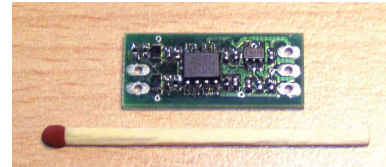
Statistische Untersuchungen zeigten bereits bei den Zufallsrohdaten keine nachweisbaren Abhängigkeiten der Zufallsbits. Eine Nachbearbeitung der Rohdaten erfolgt ausschließlich durch XOR-Verknüpfung (3fach) aufeinander folgender Zufallsbits. Zur Evaluierung der Ergebnisse des physikalischen Zufallsgenerators nach der XOR-Verknüpfung wurde eine Vielzahl von statistischen Tests auf verschiedene Bitfolgen angewendet. Keiner dieser Tests konnte Unterschiede zu einem idealen Zufallszahlen-Generator aufzeigen.

In verschiedenen Applikationen (siehe Bilder) wurden die Eigenschaften reproduzierbar, auch in großen Stückzahlen, nachgewiesen.

Bei Interesse stehen weitere Informationen zur Verfügung:

Internet: [www.ibbergmann.org](http://www.ibbergmann.org)

Email: [info@ibbergmann.org](mailto:info@ibbergmann.org)



```
*****
*
*                               AIS31 evaluation tests of raw data                               *
*
*****
```

-----  
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: 49658  
relative frequency: 0.496580  
test value: 0.00342000 < 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: 201364  
relative frequency  $v(0,1)$ : 0.495630  
relative frequency  $v(1,0)$ : 0.504980  
test value: 0.00061000 < 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: 406497  
test value  $t_1$ : 0.544544 <= 15.13  
test value  $t_2$ : 2.842726 <= 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: 821360  
test value  $t_{00}$ : 0.038724 <= 15.13  
test value  $t_{01}$ : 0.124822 <= 15.13  
test value  $t_{10}$ : 0.112510 <= 15.13  
test value  $t_{11}$ : 0.297714 <= 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: 8.00011306  
8.00011306 > 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.