

METHOD FOR TESTING A RANDOM NUMBER SOURCE AND
ELECTRONIC DEVICES COMPRISING SAID METHOD

The invention relates to a method for testing
sources generating random numbers, in particular
5 sources developed in the context of cryptographic
systems such as the random number generators
incorporated in chip cards.

It is particularly designed to be used in the
testing and validation of electronic devices such as
10 chip cards, PCMCIA's, badges, contactless cards or any
other portable apparatus.

The majority of cryptography systems of the public
key type (also referred to as asymmetric cryptography)
and secret key type (also referred to as symmetrical
15 cryptography) require the drawing of secret random
values. It is essential that such random values, or
numbers, designed to serve as keys subsequently, should
a priori be unpredictable and should not exhibit any
regularities making it possible to find them by

strategies of exhaustive or enhanced exhaustive search, in which the most probable keys are sought first.

5 In this regard, there are several methods for testing the random values generated by a random source and to ensure that the said source functions correctly and does not exhibit any drift following changes in external parameters of malevolent origin, such as alteration by induced radiation.

10 Each of these methods applies to a series, also referred to as a sequence, of integer numbers between 0 and a value d , the said series being generated by the random source.

15 The most widely known test method is the so-called "frequency" test. It is a case of counting the number of appearances of each integer between 0 and a value d in the said sequence. The number of appearances of each integer is then evaluated statistically.

20 A second so-called "series" test method consists in a counting and statistical evaluation of the number of appearances of all the possible pairs of integers between 0 and a value d . This test method can be broadened to the counting of triplets or quadruplets of integers, etc.

25 A third so-called "hole" test method exists. A hole in a sequence is a series of numbers outside a predetermined interval. It is a case of a statistical evaluation of the length of the said holes in the sequence.

30 A fourth test method, known as the "poker" test, exist. The test consists in grouping together the

numbers in the sequence in groups of five numbers and counting in each quintuplet how many different values appear.

5 A fifth test method, known as the "collection of coupons", consists of statistically evaluating the sequence size necessary for all the integer values between 0 and d to appear in the said sequence.

10 The details of these methods are found in the work by Knuth, entitled "The Art of Computer Programming, Vol. 2, Seminumerical Algorithms".

15 Another popular test method is Maurer's universal test described in the work "Journal of Cryptography", Vol. 5, N° 2, 1992, pp 89-105. This test has the advantage of revealing all the faults detectable by the test methods previously cited as well as other statistical defects not detected by these same test methods.

The so-called Maurer test method, also referred to as the universal method, comprises the following steps:

20 Step one: Generation of a sequence of $(Q+K)*L$ bits by the random source. Q , K and L are input parameters. The bits in the sequence are grouped in blocks of L bits, forming a sequence of integers between 0 and 2^L-1 of length $Q+K$. The length is stored
25 in the table $\text{block}[n]$, where n is between 1 and $Q+K$.

Step two: Calculating the test parameter, denoted f_{TU} ; this second step comprising the following steps, referred to as substeps 2.1 to 2.5:

30 2.1 Creation and initialisation of a table $\text{tab}[i]$ of size 2^L ;

2.2 For n varying from 1 to Q, making the calculation: $\text{tab}[\text{block}[n]] = n$;

2.3 Initialising the number Sum to 0;

2.4 For n varying from Q+1 to Q+K, performing the calculation:

Add $\log(n - \text{tab}[\text{block}[n]])$ to Sum;

Make the calculation: $\text{tab}[\text{block}[n]] = n$;

2.5 The parameter fTU of the test is given by:

$$\text{fTU} = (\text{Sum}/K) / \log(2);$$

Step three: Calculation of the variance per test parameter block, denoted Var. Its precise expression is given in the article published by Maurer in the work "Journal of Cryptography", Vol 5, N° 2, 1992, pp. 89-105, which is:

$$\text{Var} = (1 - z) * \sum_{i=1}^{\infty} \log 2(i)^2 * z^{i-1} - ((1 - z) * \sum_{i=1}^{\infty} \log 2(i) * z^{i-1})^2$$

with $\log 2(z) = \log(z) / \log(2)$ and $z = 1 - 2^{-L}$

Step four: Calculation of the function $c(L, K)$. An approximate expression of this function is given in the article in the abovementioned work, which is:

$$C(L, K) = 0.7 - 0.8/L + (1.6 + 12.8/L) * K^{-4/L};$$

Step five: Calculation of the standard deviation of the test parameter, denoted σ : $\sigma = c(L, K) * \sqrt{(\text{Var}/K)}$;

Step six: Calculation of the parameter y; y is determined from the rejection rate of the test fixed as an input, denoted p. Y must satisfy the equation:

$$N(-y) = p.$$

N is the normal density function described in the work by R. Langley: "Practical Statistics", Dover publications, New York, 1968. The equation $N(-y) = p$ can

be resolved using a table of values of N. Such a table is supplied in the abovementioned article.

Step seven: Calculation of the ideal mean value of the test, denoted $E[fTU]$. Its expression is given in the article published by Maurer in the work "Journal of Cryptography", Vol 5, N° 2, 1992, pp. 89-105, and is equal to:

$$E[fTU] = (1 - z) * \sum_{i=1}^{\infty} \log 2(i) * z^{i-1}$$

with $\log_2(z) = \log(z) / \log(2)$ and $z = 1 - 2^{-L}$

Step eight: Calculation of the bounds $t1$ and $t2$. They are given by the equation: $t1 = E[fTU] - y * \sigma$ and $t2 = E[fTU] + y * \sigma$.

Step nine: Result of the test.

If the test parameter fTU is between $t1$ and $t2$, then the random number generator is accepted. In the contrary case, it is refused.

The universal test method is therefore based on an approximation in the calculation of the function $c(L, K)$. This approximation makes the test less precise than is wished by the theoretical guarantee serving as a basis for it. It is possible to show that, in certain cases, the universal test proves to be 2.67 times too permissive compared with what is allowed by theory.

The object of the present invention is an improved test method for achieving the real precision guaranteed by the theoretical analysis of the universal test. This test serves notably to improve the security of portable devices of the chip card type.

The method of the invention consists in replacing step 4 of the universal test by the precise calculation of the function $c(L,K)$. This calculation is based on a probabilistic analysis of the universal test.

5 The present invention gives three distinct expressions of the function $c(L,K)$, according to the values of the parameters L and K .

The first expression of $c(L,K)$ is valid whatever the parameters L and K .

10 The second expression of $c(L,K)$ is valid in the case where the value L is between 3 and 16 and the value K is greater than $30 \cdot 2^L$, which corresponds to the most usual case of use of the test. It is much more simple to calculate than the first expression and can
15 therefore be effected on a simple microcontroller in a few milliseconds.

The third expression of $c(L,K)$ is valid for a value of $L > 16$ and a value of $K > 30 \cdot 2^L$. This expression is even more simple to calculate.

20 The first expression of $c(L,K)$ can be obtained by means of the method described below, which contains nine steps:

1. Calculation of: $u = 1 - 2^{-L}$ and $v = 1 - 1/(2^L - 1)$;
 u and v being real numbers;
- 25 2. Creation of two tables $tab1$ and $tab2$ of size $60 \cdot 2^L$;
3. Filling of $tab1$ and $tab2$: for this purpose,
 3.1 Execute $z = u$, $sum = 0$, $z1 = 1$;

3.2 For i ranging from 1 to $30 \cdot 2^L$, repeating the two operations which are: add $\log_2(i) \cdot z_1$ to sum, in which $\log_2$ designates the logarithm to base 2, and

calculate: $z_1 = z_1 \cdot z$;

5 3.3 Execute $\text{tab1}[0] = (1 - z) \cdot \text{sum}$;

3.4 For i ranging from 1 to $60 \cdot 2^L$,

Execute $\text{tab1}[i] = (\text{tab1}[i-1] - (1 - z) \cdot \log_2(i)) / z$;

3.5 Repeat steps 3.1, 3.2, 3.3, 3.4, replacing u with v and tab1 with tab2 ;

10 4. Calculation of the variance per block denoted Var ;

4.1 Execute $\text{sum} = 0$ and $x = 1$;

4.2 For i varying from 1 to $30 \cdot 2^L$, execute the following two operations:

15 Add $\log_2(i)^2 \cdot x$ to sum and

Execute $x = x \cdot z$;

4.3 Make $\text{Var} = \text{sum} / 2^L - \text{tab1}[0]^2$;

5. Calculation of $P(K)$;

5.1 Make $\text{sum} = 0$ and $x = 1$;

20 5.2 For i varying from 1 to $30 \cdot 2^L$: carry out the following three operations:

Calculate $y = u^2 \cdot (\text{tab2}[i+K-1] - \text{tab1}[i+K]) \cdot (\text{tab2}[0] - v^i \cdot \text{tab2}[i]) + u \cdot \text{tab1}[0] \cdot (\text{tab1}[i+K-1] - \text{tab2}[i+K-1])$,

Add $y \cdot x$ to sum,

25 Execute $x = x \cdot u$;

5.3 Execute $P(K) = u^{(K-1)} \cdot \text{sum}$;

6. Calculation of $P(1)$:

Same method as at step 5, replacing K with 1;

7. Calculation of $Q(K)$:

30 7.1 Make $\text{sum} = 0$, $\text{sum2} = 0$ and $x = 1$,

7.2 For i varying from 1 to $30 \cdot 2^L$:

Add $i \cdot \log_2(i) \cdot u^{(i-2)}$ to sum2 ;

Execute the following three operations:

Calculate $y = u^2 \cdot (\text{tab2}[i+K-1] -$

5 $\text{tab1}[i+K]) \cdot ((i+k) \cdot \text{tab2}[0] - v^i \cdot \text{tab2}[i]) - 2^{(-L)} \cdot \text{sum2}) + u \cdot (i+K-1) \cdot \text{tab1}[0] \cdot (\text{tab1}[i+K-1] - \text{tab2}[i+K=1]),$

Add $y \cdot x$ to sum ,

Execute $x = x \cdot u$;

7.3 Execute $Q(K) = u^{(K-1)} \cdot \text{sum}$

10 8. Calculation of $Q(1)$

Same method as at step 7, replacing K with 1

9. Calculation of $c(L, K)$

$c(L, K) = \sqrt{(1 - 2/\text{Var} \cdot (P(1) - P(K) - (Q(1) - Q(K))/K)}$

15 The second expression of $c(L, K)$ is valid for $K > 30 \cdot 2^L$. It is calculated according to the following method in two steps:

Step one: Reading of the values of $e(L)$ and $d(L)$, e and d being real values, listed in the following table, for L between 3 and 16:

20

L	d(L)	e(L)
3	0.2732725	0.4890883
4	0.3045101	0.4435381
5	0.3296587	0.4137196
6	0.3489769	0.3941338
7	0.3631815	0.3813210
8	0.3732189	0.3730195
9	0.3800637	0.3677118
10	0.3845867	0.3643695
11	0.3874942	0.3622979

12	0.3893189	0.3610336
13	0.3904405	0.3602731
14	0.3911178	0.3598216
15	0.3915202	0.3595571
16	0.3917561	0.3594040

Step two: Calculate the value $c(L,K)$ using the formula:

$$c(L,K) = \sqrt{(d(L) + e(L) * 2^L / K)}$$

5 The third expression of $c(L,K)$ is valid for $L > 16$ and $K > 30 * 2^L$. It is given by the following formula:

$$c(L,K) = \sqrt{(1 - 6/\Pi^2 + 2/\Pi^2 * (4 * \log(2) - 1) * 2^L / K)}$$

The present invention also relates , as stated at the beginning of the description, page 1, to an
 10 electronic device which is not depicted by a figure or diagram. This electronic device is a device for the automatic verification of the physical integrity of a self-checking integrated circuit checking the integrity of its random generator from the three variants of the
 15 method of the invention, also described above, or more explicitly from the three distinct expressions of the function $c(L,K)$, in order to ensure that the said generator is functioning correctly in general and does not exhibit any drift following changes in external
 20 parameters of malevolent origin, such as an alteration by induced radiation, in particular.

Preferentially, the electronic device carrying out the test is a portable device, and more particularly consists, for example, of a chip card, a contactless
 25 card, a PCMCIA card, a badge or an intelligent watch.

Finally, the electronic device of the invention can be an external device consisting of a machine or installation designed to test the correct functioning of random generators incorporated in the said portable devices. This external device allows an exchange of information with the portable device so as to check that the random generator is functioning correctly. The external device interacts with the portable device in order to check the integrity of its random generator.



CLAIMS

1. A method for testing sources of random numbers, comprising the following steps:

5 Step one: Generation of a sequence of $(Q+K)*L$ bits by the random source, Q , K and L being input parameters, the bits in the sequence being grouped in blocks of L bits, forming a sequence of integers between 0 and 2^L-1 of length $Q+K$, the length being
10 stored in the table $\text{block}[n]$, where n is between 1 and $Q+K$;

Step two: Calculating the test parameter, denoted fTU ; this second step comprising the following steps, referred to as substeps 2.1 to 2.5:

15 2.1 Creation and initialisation of a table $\text{tab}[i]$ of size 2^L ;

2.2 For n varying from 1 to Q , making the calculation: $\text{tab}[\text{block}[n]] = n$;

2.3 Initialising the number Sum to 0;

20 2.4 For n varying from $Q+1$ to $Q+K$, performing the calculation in two operations:

Add $\log(n - \text{tab}[\text{block}[n]])$ to Sum ;

Make the calculation: $\text{tab}[\text{block}[n]] = n$;

2.5 The parameter fTU of the test is given by:

25 $\text{fTU} = (\text{Sum}/K) / \log(2)$;

Step three: Calculation of the variance per test parameter block, denoted Var , from the following expression:

$$\text{Var} = (1 - z) * \sum_{i=1}^{\infty} \log 2(i) z^{i-1} - ((1 - z) * \sum_{i=1}^{\infty} \log 2(i) * z^{i-1})^2$$



with $\log_2(z) = \log(z)/\log(2)$ and $z = 1 - 2^{-L}$

Step four: Calculation of the function $c(L, K)$;

Step five: Calculation of the standard deviation of the test parameter, denoted σ : $\sigma = c(L, K) * \sqrt{\text{Var}/K}$;

5 Step six: Calculation of the parameter y ; y is determined from the rejection rate of the test fixed as an input, denoted p . Y must satisfy the equation:

$$N(-y) = p,$$

N is the normal density function;

10 Step seven: Calculation of the ideal mean value of the test, denoted $E[\text{fTU}]$, given by the following formula:

$$E[\text{fTU}] = (1 - z) * \sum_{i=1}^{\infty} \log_2(i) * z^{i-1}$$

with $\log_2(z) = \log(z)/\log(2)$ and $z = 1 - 2^{-L}$

15 Step eight: Calculation of the bounds t_1 and t_2 . They are given by the equation: $t_1 = E[\text{fTU}] - y * \sigma$ and $t_2 = E[\text{fTU}] + y * \sigma$;

20 Step nine: Result of the test: the random number generator being accepted if the test parameter fTU is between t_1 and t_2 , and rejected in the contrary case,

the said method being characterised in that step four consists of a calculation of the function $c(L, K)$ which is valid whatever the parameters L and K .

25 2. A method for testing sources of random numbers according to Claim 1, characterised in that step four consists of a calculation of the function $c(L, K)$ which is valid in the case where the value of L is between 3 and 16 and the value of K is greater than $30 * 2^L$.



3. A method for testing sources of random numbers according to Claim 1, characterised in that step four consists of a calculation of the function $c(L,K)$ which is valid for a value of $L > 16$ and a value of $K > 30 \cdot 2^L$.

5 4. A method according to Claim 1, characterised in that the calculation of the function $c(L,K)$ contains nine steps:

1. Calculation of: $u = 1 - 2^{-L}$ and $v = 1 - 1/(2^L - 1)$;
 u and v being real numbers;
 10 2. Creation of two tables $tab1$ and $tab2$ of size $60 \cdot 2^L$;

3.1 Execute $z = u$, $sum = 0$, $z1 = 1$;
 3.2 For i ranging from 1 to $30 \cdot 2^L$, repeating the two operations which are: add $\log_2(i) \cdot z1$ to sum , in
 15 which $\log_2$ designates the logarithm to base 2, and calculate: $z1 = z1 \cdot z$;

3.3 Execute $tab1[0] = (1 - z) \cdot sum$;
 3.4 For i ranging from 1 to $60 \cdot 2^L$,
 Execute $tab1[i] = (tab1[i-1] - (1 - z) \cdot \log_2(i)) / z$;
 20 3.5 Repeat steps 3.1, 3.2, 3.3, 3.4, replacing u with v and $tab1$ with $tab2$;

4. Calculation of the variance per block denoted Var ;

4.1 Execute $sum = 0$ and $x = 1$;
 25 4.2 For i varying from 1 to $30 \cdot 2^L$, execute the following two operations:

Add $\log_2(i)^2 \cdot x$ to sum and
 Execute $x = x \cdot z$;

4.3 Make $Var = sum / 2^L - tab1[0]^2$;

30 5. Calculation of $P(K)$;



5.1 Make $\text{sum}=0$ and $x=1$;

5.2 For i varying from 1 to $30 \cdot 2^L$: carry out the following three operations:

5 Calculate $y: y = u^2 \cdot (\text{tab2}[i+K-1] - \text{tab1}[i+K]) \cdot (\text{tab2}[0] - v^i \cdot \text{tab2}[i]) + u \cdot \text{tab1}[0] \cdot (\text{tab1}[i+K-1] - \text{tab2}[i+K-1])$,

Add $y \cdot x$ to sum ,

Execute $x = x \cdot u$;

5.3 Execute $P(K) = u^{(K-1)} \cdot \text{sum}$;

6. Calculation of $P(1)$:

10 Same method as at step 5, replacing K with 1;

7. Calculation of $Q(K)$:

7.1 Make $\text{sum}=0$, $\text{sum2}=0$ and $x=1$,

7.2 For i varying from 1 to $30 \cdot 2^L$:

Add $i \cdot \log_2(i) \cdot u^{(i-2)}$ to sum2 ;

15 Execute the following three operations:

Calculate $y = u^2 \cdot (\text{tab2}[i+K-1] - \text{tab1}[i+K]) \cdot ((i+k) \cdot \text{tab2}[0] - v^i \cdot \text{tab2}[i]) - 2^{(-L)} \cdot \text{sum2} + u \cdot (i+K-1) \cdot \text{tab1}[0] \cdot (\text{tab1}[i+K-1] - \text{tab2}[i+K-1])$,

Add $y \cdot x$ to sum ,

20 Execute $x = x \cdot u$;

7.3 Execute $Q(K) = u^{(K-1)} \cdot \text{sum}$

8. Calculation of $Q(1)$

Same method as at step 7, replacing K with 1

9. Calculation of $c(L, K)$

25 $c(L, K) = \sqrt{(1 - 2/\text{Var} \cdot (P(1) - P(K) - (Q(1) - Q(K)) / K)}$

5. A method according to Claim 2, characterised in that the function $c(L, K)$ contains two steps:

30 Step one: Reading of the values of $e(L)$ and $d(L)$, e and d being real values, listed in the following table, for L between 3 and 16:



L	d(L)	e(L)
3	0.2732725	0.4890883
4	0.3045101	0.4435381
5	0.3296587	0.4137196
6	0.3489769	0.3941338
7	0.3631815	0.3813210
8	0.3732189	0.3730195
9	0.3800637	0.3677118
10	0.3845867	0.3643695
11	0.3874942	0.3622979
12	0.3893189	0.3610336
13	0.3904405	0.3602731
14	0.3911178	0.3598216
15	0.3915202	0.3595571
16	0.3917561	0.3594040

Step two: Calculate the value $c(L,K)$ using the formula:

$$c(L,K) = \sqrt{(d(L) + e(L) * 2^L / K)}$$

6. A method according to Claim 3, characterised in that the calculation of the functions $c(L,K)$ is effected by means of the following formula:

$$c(L,K) = \sqrt{(1 - 6/\Pi^2 + 2/\Pi^2 * (4 * \log(2) - 1) * 2^L / K)}$$

7. An electronic device for the self-checking of the physical integrity of a self-checking integrated circuit and checking the integrity of its random generator, in order to ensure that the latter is functioning correctly in general and does not exhibit any drift following changes in external parameters of



malevolent origin such as an alteration by induced radiation, in particular, according to any one of Claims 1 to 3.

5 8. An electronic device according to Claim 7, characterised in that the device performing the test is a portable device.

9. An electronic device according to Claim 8, characterised in that the device is a chip card, a contactless card, a PCMCIA card, a badge or an
10 intelligent watch.

10. An electronic device according to any one of Claims 1 to 6, characterised in that an external device performing the test consists of a machine or installation designed to test the correct functioning
15 of random generators incorporated in the said portable devices.