GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

File No.: 62997-2018

GM/T 0062-2018

Random number test requirements for cryptographic modules

密码产品随机数检测要求

Issued on: May 02, 2018 **Implemented on: May 02, 2018**

Issued by: State Cryptography Administration

Table of Contents

Random number test

requirements for cryptographic modules

1 Scope

This Standard specifies the randomness test index and test requirements for random number generators to generate random numbers in the application of cryptographic products.

This Standard applies to the test of random number generators, and can also guide the development of random number generators.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 32915 Information security technology - Randomness test methods for binary sequence

3 Terms, definitions and symbols

3.1 Terms and definitions

For the purpose of this document, the terms and definitions given in GB/T 32915 and the following apply.

3.1.1

sample test

Product randomness test of manufacturer's product samples, carried out by a third-party test organization.

3.1.2

delivery test

Product random number function and quality test that is carried out by the

The main feature of Class B products is that they are powered on when used; the random number test and processing capability is limited; there are strict requirements for power-on response speed. Typical product form is IC card.

The main feature of Class C products is that they are powered on when used; the random number test and processing capability is limited; there is no strict requirement for power-on response speed. Typical product form is USBKey.

The main feature of Class D products is that they are powered on for the long term; the random number test and processing capability is limited; there is no strict requirement for power-on response speed. Typical product form is POS machine.

The main feature of Class E products is that they are powered on for the long term; the random number test and processing capability is strong; there is no requirement for power-on response speed. Typical product form is server.

This Standard proposes the random number test requirements for each product form.

4.2 Application phase division

This Standard divides the random number test into four different application phases: sample test, delivery test, power on test and running test.

For the above 4 application phases, this Standard specifies the corresponding random number test method.

4.3 Data format

The data to be tested is tested in the form of a binary sequence.

4.4 Test items

The randomness test items used in this Standard involve 15 items specified in GB/T 32915, which are single-bit frequency test, intra-block frequency test, poker test, overlapping sub-sequence test, total run test, run distribution test, intra-block maximum run test, binary derivation test, autocorrelation test, matrix rank test, accumulate sum test, approximate entropy test, linear complexity test, general statistical test, discrete Fourier test.

4.5 Significance level

The significance level used in this Standard is $a = 0.01$.

4.6 Parameter setting

In this Standard, for different application phases of different product forms, the

a) Test amount: The sample length shall not be less than 128 bits.

b) Test item: Single-bit frequency test or poker test. The poker test parameter m = 2.

c) Test determination criteria: If the tested sequence does not pass the test criteria, the test is unqualified. It is allowed to repeat the random number collection and test once. If the repeated test is still unqualified, it is determined that the random number generator of the product is invalid.

6.3 Power on test

It is not required in this Standard.

6.4 Running test

6.4.1 Cyclical test

It is not required in this Standard.

6.4.2 Single test

The running single test of random numbers includes the following requirements:

a) Test amount: It is determined according to the size of the random number collected each time in the actual application, but the length shall not be less than 256 bits, and the unused sequence that has passed the test can continue to be used.

b) Test item: Poker test, parameter m = 2.

c) Test determination criteria: If the tested sequence does not pass the test criteria, the test is unqualified. It is allowed to repeat the random number acquisition and test once. If the repeated test is still unqualified, it is determined that the random number generator of the product is invalid.

7 Random number test for Class C products

7.1 Sample test

Carry out the random number test according to GB/T 32915.

7.2 Delivery test

The delivery test of random numbers includes the following requirements:

a) Test amount: The sample length shall not be less than 256 bits.

8 Random number test for Class D products

8.1 Sample test

Carry out the random number test according to GB/T 32915.

8.2 Delivery test

The delivery test of random numbers includes the following requirements:

a) Test amount: The sample length shall not be less than 256 bits.

b) Test item: Single-bit frequency test or poker test. The poker test parameter $m = 2$.

c) Test determination criteria: If the tested sequence does not pass the test criteria, the test is unqualified. It is allowed to repeat the random number collection and test once. If the repeated test is still unqualified, it is determined that the random number generator of the product is invalid.

8.3 Power on test

The power on test of random numbers includes the following requirements:

a) Test amount: 20×10^4 bit random numbers are collected and divide into 20 groups of 10^4 bits each.

b) Test item: Poker test, parameter $m = 2$.

c) Test determination criteria: If 2 or more groups of the tested sequence does not pass the test criteria, the test is unqualified. It is allowed to repeat the random number collection and test once. If the repeated test is still unqualified, it is determined that the random number generator of the product is invalid.

8.4 Running test

8.4.1 Cyclical test

The running cyclical test of random numbers includes the following requirements:

a) Test amount: 5×10^4 bit random numbers are collected and divided into 5 groups of 10^4 bits each.

b) Test item: Poker test, parameter $m = 2$.

9.3 Power on test

The power on test of random numbers includes the following requirements:

a) Test amount: 20×10^6 bit random numbers are collected and divided into 20 groups of 10^6 bits each.

b) Test items: Test according to the test items specified in GB/T 32915.

c) Test determination criteria: If 2 or more groups of the tested sequence does not pass the test criteria, the test is unqualified. It is allowed to repeat the random number collection and test once. If the repeated test is still unqualified, it is determined that the random number generator of the product is invalid.

9.4 Running test

9.4.1 Cyclical test

The running cyclical test of random numbers includes the following requirements:

a) Test amount: 4×10^5 bit random numbers are collected and divided into 20 groups of 2×10^4 bits each.

b) Test items: The collected random numbers are tested according to the 12 items in GB/T 32915, except for discrete Fourier test, linear complexity test, and general statistical test.

c) Test determination criteria: If 2 or more groups of the tested sequence does not pass the test criteria, the test is unqualified. It is allowed to repeat the random number collection and test once. If the repeated test is still unqualified, it is determined that the random number generator of the product is invalid.

d) Test period: Configurable, the test interval is no longer than 12 h.

9.4.2 Single test

The running single test of random numbers includes the following requirements:

a) Test amount: It is determined according to the size of the random number collected each time in the actual application, but the length shall not be less than 256 bits, and the unused sequence that has passed the test can continue to be used.

b) Test item: Poker test, parameter $m = 2$.

This is an excerpt of the PDF (Some pages are marked off intentionally)

Full-copy PDF can be purchased from 1 of 3 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

3. https://www.google.com/search?tbm=bks&q=ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Google Books -- Select your currency.
- Processed by Google (delivery, tax invoice etc.). Delivered in 9 seconds by Google.
- Tips: Download an unprotected True-PDF (text-editable) from Google-Books:
  1. https://play.google.com/books → 2. Sign in → Google account
  3. Find the BOOK you bought → 4. Click "3-dots" → Export
  5. Save as "*.pdf" (Save True-PDF to your local computer for offline reading/printing)

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

Accountable person and shareholder: Wayne Zheng

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

------ The End ------