Chinastandards.org

ICS 35.040
CCS L 80

GM

GM/T 0078-2020

The design guidelines for cryptographic random number generation module

密码随机数生成模块设计指南

(English Translation)

Issued on: December 28, 2020 **Implemented on: July 1, 2021**

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0078-2020

Chinastandards.org

Table of Contents

Foreword 1
Scope 2
Normative References 3
Terms and Definitions 4
Random Number Generation Module 5
Thermal Noise 6
Abbreviations 7
General Model of Random Number Generation Module 8
Typical model of principle 9
Example of circuit 10
Typical model of principle 11
Random bit generation rate 12
Typical model of principle 13
Thermal noise amplitude 14
Failure Detection of Physical Random Sources 15
Randomness Detection of Physical Random Sources 16
Design Requirements for Post-processing Algorithm 17
Post-processing algorithm based on hash functions 18
Post-processing algorithm based on m-sequence 19
XOR chain method 20
Odd-even grouping method 21
M-LSB method 22
Foreword 23
Design Requirements for Post-processing Algorithm 24
Post-processing algorithm based on hash functions 25
Post-processing algorithm based on m-sequence 26
XOR chain method 27
Odd-even grouping method 28
M-LSB method 29

Preview: page 2 of 5 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0078-2020

Foreword

This Standard was drafted in accordance with the rules in GB/T 1.1-2020 Directives for Standardization - Part 1: Rules for the Structure and Drafting of Standardizing Documents.

Please be noted that certain content of this document might involve patents. The institution issuing this document does not undertake the responsibility of identifying these patents.

This Standard was proposed by and shall be under the jurisdiction of Cryptography Standardization Technical Committee.

1 Scope

This Standard specifies the design requirements for cryptographic hardware random number generation module.

This Standard is applicable to the guidance on the research, development and test of random number generation module.

2 Normative References

The content of the following documents constitutes indispensable clauses of this document through normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GM/T 0005 Randomness Test Specification GM/T 0008 Cryptography Test Criteria for Security IC

3 Terms and Definitions

What is defined in GM/T 0005 and GM/T 0008, and the following terms and definitions are applicable to this document.

3.1 Random Number Generation Module

Random number generation module refers to a circuit that utilizes the natural randomness of the real world to extract random quantities from random physical processes and undergoes transformation processing to output random numbers.

3.2 Thermal Noise

Thermal noise, which is also known as white noise, is caused by thermal vibration of electrons in the conductor. It exists in all electronic devices and transmission media. It is the result of temperature changes but is not affect by frequency changes. Thermal noise is

Preview: page 3 of 5 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0078-2020

distributed in the same form in all frequency spectra, and it cannot be eliminated.

4 Abbreviations

The following abbreviations are applicable to this document.

CBC. Cipher Block Chaining

5 General Model of Random Number Generation Module

The general model of random number generation module is shown in Figure 1.

The random number generation module has two outputs, one is the random number sequence output, and the other is the random source detection output that provides detection. The randomness of the output random number sequence shall comply with the stipulations of GM/T 0005.Random source detection output is mainly used to detect the basic randomness of physical random sources.

6.1.1 Typical model of principle

Utilizing the characteristics of chaotic function to design a chaotic system is to take random noise as minor disturbance of the chaotic system. Since the output of the system is affected by the random noise in the system, the output sequence of the system is unpredictable, and random sequence may be generated. The realization of the physical random sources based on the principle of the chaotic dynamical system mainly considers the circuit realization of the chaotic function and the realization of random noise.

6.1.4 Example of circuit

A circuit example of physical random sources based on the principle of discrete chaotic Sampling

6.2.1 Typical model of principle

The method of utilizing phase jitter to generate random numbers has been extensively applied and can be conveniently designed and implemented in both digital and analog circuits.

6.2.2.1 Random bit generation rate

In circuit design, the sampling clock is a slow clock signal. The sampling frequency of the sampling clock determines the rate of random bit sequence generation.

Preview: page 4 of 5 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0078-2020

6.3.1 Typical model of principle

The principle of direct thermal noise amplification is to adopt an amplifying circuit to directly amplify the thermal noise in the circuit, and then, output a random source sequence through comparison.

6.3.2.1 Thermal noise amplitude

Resistor thermal noise is one of the important modes to design noise source. In terms of the resistor thermal noise source, its thermal noise is only related to temperature and resistance value; it has nothing to do with the passed current. Its unilateral spectral density S(f) is shown in Formula (2); the noise power Vn2 is shown in Formula (3).

7 Failure Detection of Physical Random Sources

The failure detection of physical random sources is to detect the final output sequence of the circuit part of the physical random sources when the random number generation module is working.

8 Randomness Detection of Physical Random Sources

The randomness detection of physical random sources is to detect the output signal of the physical random sources before post-processing when the random number generation module is working.

9.1 Design Requirements for Post-processing Algorithm

The basic principle of the post-processing algorithm is that the average entropy per bit cannot be reduced. In other words, the post-processing module inputs n bits and outputs m bits, and it must be guaranteed that n >= m, in which, the premise of n = m is that the output sequence of the physical random sources passes the detection by GM/T 0005.

9.2.2 Post-processing algorithm based on hash functions

The post-processing algorithm based on hash functions needs to adopt approved secure hash functions.

9.2.3 Post-processing algorithm based on m-sequence

The post-processing is realized by m-sequence with a length of K through linear feedback shift register or non-linear feedback shift register. The input of the physical random sources is synchronized with the cyclic shift of the shift register, and the feedback bit and the current bit of the digitized noise signal are XORed and output.

The m-sequence method shall satisfy the following requirements.

Preview: page 5 of 5 shown, 16 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0078-2020