

ICS 35.030
CCS L 80

GM

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GM/T 0103-2021

General framework of random number generator

随机数发生器总体框架

(English Translation)

Issued on: October 18, 2021

Implemented on: May 1, 2022

Issued by: State Administration of Cryptography

Table of Contents

Foreword	1
Scope	2
Normative references	3
Terms and definitions	4
Overview	5
Entropy	6
Entropy evaluation	7
Post-processing	8
Testing	9
Foreword	10
Overview	11
Entropy	12
Entropy evaluation	13
Post-processing	14
Testing	15

Foreword

This document was drafted in accordance with the provisions of GB/T 1.1-2020 "Directives for standardization - Part 1: Rules for the structure and drafting of standardizing documents".

Please note that some contents of this document may refer to patents. The issuing agency of this document assumes no responsibility for identifying patents.

This document was proposed by AND shall be under the jurisdiction of the Encryption Industry Standardization Technical Committee.

Drafting organizations of this document. Beijing Hongsi Electronic Technology Co., Ltd., Beijing Zhixin Microelectronics Technology Co., Ltd., Data and Communication Protection Research and Education Center of the Chinese Academy of Sciences, Taiyuan University of Technology, University of Science and Technology Guodun Quantum Technology Co., Ltd., Anhui Jiantian Quantum Technology Co., Ltd., The 30th Research Institute of China Electronics Technology Group Corporation, Commercial Encryption Testing Center of the State Encryption Administration.

1 Scope

This document is an overall upper standard for random number generator design; it specifies the overall framework for random number generator design.

This document is applicable to the research, development, and testing of random number generators. It can also promote the formulation of relevant standards for random number generators.

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text. Among them, for dated references, only the version corresponding to the date is applicable to this document; for undated references, the latest version (including all amendments) is applicable to this document.

GB/T 25069 Information security technology - Glossary GB/T 32915 Information security technology - Binary sequence randomness detection method GM/T 0062 Random number test requirements for cryptographic modules GM/T 0078-2020 The design guidelines for cryptographic random number generation module GM/T 0105 Design guide for software-based random number generators GM/Z 4001 Cryptographic terminology

3 Terms and definitions

The terms and definitions as defined in GB/T 25069, GB/T 32915, GM/T 0062, GM/T 0078, GM/T 0105, GM/Z 4001, as well as the following terms and definitions, apply to this document.

Entropy source

A component, device, or event that produces an output. When this output is captured and processed in some way, a bitstring containing an entropy is produced.

[Source. GB/T 25069-2010, 2.1.31] 3.2 Thermal noise Typically unwanted, but inherently generated spurious electrical signals (also known as "white noise") in components (such as operational amplifiers, reverse-biased diodes, or resistors).

Note: Usually every effort is made to minimize this phenomenon. However, the unpredictability of this phenomenon can be exploited as a source of entropy, in random bitstream generation.

[Source. GB/T 25069-2010, 2.2.4.8] 3.3 Chaotic oscillation the complex and disordered oscillation state of a nonlinear system.

Note: Rooted in the local instability of the system, it manifests as initial value sensitivity and inherent randomness.

Phase jitter

Rapid, short-term, random fluctuations in wave phase, which is caused by temporal instabilities.

4.1 Overview

The random number generator's design framework is as shown in Figure 1. The random number generator usually includes entropy source, post-processing, testing. In the design stage, entropy evaluation is performed on the entropy source or random source sequence, whilst in the product testing and use phase, the validity test or randomness test is performed on the random source sequence or random number sequence.

4.2 Entropy

The entropy source obtains a random source sequence, by sampling and quantifying the uncertainty in components, equipment or events.

4.3 Entropy evaluation

The entropy evaluation predicts and evaluates the random source sequence, through theoretical modeling analysis, statistical testing and other methods, to obtain the entropy estimate.

4.4 Post-processing

The post-processing module processes the random source sequence; generates a random number sequence, that meets the statistical testing, through a post-processing algorithm.

4.5 Testing

The testing module performs failure inspection or randomness inspection, on the random source sequence or random number sequence, to ensure the functional correctness and quality safety of the random number generator.

Appendix A

(Informative)

Standard system framework of random number generator this Appendix gives the framework of the random number generator standard system, as shown in Figure A.1, which can be divided into framework standards, design standards, testing standards.

GM/T 0103-2021

CRYPTOGRAPHY INDUSTRY STANDARD ICS 35.030 CCS L 80 General framework of random number generator Issued on. OCTOBER 18, 2021 Implemented on. MAY 01, 2022 Issued by. National Cryptography Administration

Table of Contents

Foreword...	3
1 Scope...	4
2 Normative references...	4
3 Terms and definitions...	4
4 Overall framework of random number generator design...	6
4.1 Overview...	6
4.2 Entropy...	7
4.3 Entropy evaluation...	8
4.4 Post-processing...	8
4.5	
Testing...	9
Appendix A (Informative) Standard system framework of random number generator	10
References...	12

Foreword

This document was drafted in accordance with the provisions of GB/T 1.1-2020 "Directives for standardization - Part 1: Rules for the structure and drafting of standardizing documents".

Please note that some contents of this document may refer to patents. The issuing agency of this document assumes no responsibility for identifying patents.

This document was proposed by AND shall be under the jurisdiction of the Encryption Industry Standardization Technical Committee.

Drafting organizations of this document. Beijing Hongsi Electronic Technology Co., Ltd., Beijing Zhixin Microelectronics Technology Co., Ltd., Data and Communication Protection Research and Education Center of the Chinese Academy of Sciences, Taiyuan University of Technology, University of Science and Technology Guodun Quantum Technology Co., Ltd., Anhui Jiantian Quantum Technology Co., Ltd., The 30th Research Institute of China Electronics Technology Group Corporation, Commercial Encryption Testing Center of the State Encryption Administration.