

ICS 35.030
CCS L 80

GM

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

GM/T 0105-2021

Design guide for software-based random number generators

软件随机数发生器设计指南

(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
Entropy	5
Entropy source	6
Known-answer test	7
Entropy pool	8
Min-entropy	9
Random number generator; RNG	10
Abbreviated Terms	11
Basic model	12
Entropy pool	13
Entropy estimation	14
Health test	15
Internal state	16
DRNG self-test	17
Overview	18
Security-Level-1 in GB/T 37092	19
Security-Level-2 in GB/T 37092	20
General	21
Exclusiveness of entropy source	22
Foreword	23
General	24
Exclusiveness of entropy source	25

Foreword

This Document was drafted as per the rules specified in GB/T 1.1-2020 Directives for Standardization - Part 1: Rules for the Structure and Drafting of Standardizing Documents.

Please note some contents may involve patents. The issuing agency of this Document shall not assume the responsibility to identify these patents.

This Document was proposed by and under the jurisdiction of Cryptography Standardization Technical Committee.

Drafting organizations of this Document. Data Assurance and Communication Security Research Center, Chinese Academy of Sciences; Institute of Software, Chinese Academy of Sciences; Zhejiang University; Shenzhen Technology University; Shenzhen New Creation Xin'an Science and Technology Co., Ltd.; Westone Information Industry INC.; School of Cyber Science and Technology, University of Science and Technology of China; Chengdu University of Information Technology; China Financial Certification Authority; Beijing Hongsi Electronic Technology Co., Ltd.; Beijing Smartchip Microelectronics Technology Co., Ltd.; and ZhiXun Crypto (Shanghai) Testing and Evaluation Technology Co., Ltd.

Chief drafting staffs of this Document. Ma Yuan, Lv Na, Chen Hua, Shen Haibin, Zheng Fangyu, Chen Tianyu, Zhang Yiwei, Fan Junfeng, Lin Jingqiang, Liu Pan, Wu Xinying, Zhang Liting, Wu Zhen, Wang Feiyu, Zhang Wenjing, Hu Xiaobo, Fan Limin, and Han Wei.

1 Scope

This Document provides the basic model for the design of software random number generator, the design guidelines for basic components, and the security classification method. In the appendix, design examples based on the SM3 algorithm and the SM4 algorithm are given.

This Document is applicable to the design, development, testing and evaluation of software random number generators.

2 Normative References

The provisions in following documents become the essential provisions of this Document through reference in this Document. For the dated documents, only the versions with the dates indicated are applicable to this Document; for the undated documents, only the latest version (including all the amendments) is applicable to this Document.

GB/T 15852.1 Information technology - Security techniques - Message authentication codes -Part 1: Mechanisms using a block cipher
GB/T 17964 Information security technology - Modes of operation for a block cipher
GB/T 32905 Information security technology - SM3 cryptographic hash algorithm
GB/T 32907 Information security technology - SM4 block cipher algorithm
GB/T 32915-2016 Information security technology - Binary sequence randomness detection method

3 Terms and Definitions

For the purposes of this Document, the terms and definitions given in GB/T 32915-2016, GB/T 37092-2018 and GM/Z 4001 and the following apply.

3.1 Entropy

A measure of the disorder, randomness or variability of a closed system.

3.2 Entropy source

A component, device, or event that produces an output. When captured and processed in some way, produces a string of bits containing entropy.

3.3 Known-answer test

A method of testing a deterministic mechanism by having the mechanism process a given input and then compare the resulting output with a known value.

3.4 Entropy pool

A storage area for temporarily saving entropy.

3.5 Min-entropy

The lower bound of entropy is an estimate of the worst-case entropy of a given sample.

NOTE: If k is the maximum value such that $P(X = x) \leq 2^{-k}$, then the minimum entropy of a bit string X (or more precisely, the corresponding random variable that forms such a random bit string) is k . That is, X contains at least k bits of entropy or randomness.

3.6 Random number generator; RNG

A device or program that generates a random binary sequence.

[SOURCE. GB/T 32915-2016, 2.2]

4 Abbreviated Terms

The following abbreviated terms apply to this Document.

CPU. Central Processing Unit;

RNG. Random Number Generator;

5.1 Basic model

The basic model of the software random number generator given in this Document is shown in

Figure 1, which mainly includes system entropy source, entropy estimation, entropy pool, DRNG and health test, etc. Among them, DRNG is mainly composed of basic components such as internal state, initialization function, reseed function, output function, self-test, etc.

5.3 Entropy pool

The entropy pool is an important component in the software random number generator to ensure entropy collection. When idle, the RNG can collect the entropy source output; when needed, the required data can be read from the entropy pool in time, thereby reducing the delay in generating random numbers. In addition, in order to increase the obfuscation of entropy source data and save entropy pool space, an iterative compression function can be used in the entropy pool to increase the entropy rate, such as realized through a circular shift register.

5.4 Entropy estimation

Entropy estimation is the key to ensuring the security of the random number generator. The system entropy source is generally a non-physical entropy source, so it is difficult to establish a reliable mathematical model to characterize the random behavior of the entropy source, and it is also difficult to further estimate the entropy of the entropy source through theoretical modeling methods.

5.5 Health test

Health test is used to monitor the status of the entropy source to ensure the safety of the random number generator during operation. Health test includes power-on health test, continuous health test and on-demand health test.

5.6.2 Internal state

The internal state of DRNG can be regarded as the internal (temporary) storage of the software random number generator, which consists of all parameters, variables and other stored values used or executed by DRNG. The internal state of DRNG includes.

5.6.6 DRNG self-test

Similar to the self-test of the cryptographic module in GB/T 37092-2018, DRNG also needs to perform self-test to ensure that the designed DRNG can continue to operate correctly in the way designed and implemented.

6.1 Overview

Since the security protection requirements of cryptographic modules at different levels are different, this Document provides a grading method for software random number generators in cryptographic modules that meet the security level 1 and security level 2 of GB/T 37092-2018 for the DRNG reseeding mechanism, considering the duration and number of times the seed is used.