Chinastandards.org

ICS 35.040
CCS L 80

GM

GM/T 0083-2020

Guideline for the mitigation of non-invasive attacks against cryptographic modules

密码模块非入侵式攻击缓解技术指南

(English Translation)

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

Issued by: State Administration of Cryptography

Preview: page 1 of 4 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0083-2020

Chinastandards.org

Table of Contents

1 Scope
2 Normative references
3 Terms and definitions
4 Symbols and abbreviations
4.1 Symbol
4.2 Abbreviations
5 Non-invasive attack methods
5.1 Overview
5.2 Naming and Classification
5.3 Analysis Process
5.4 Relevance to safety functions
6 Non-invasive attack mitigation techniques
6.1 Overview
6.2 Timing analysis attack mitigation technology
6.3 Energy analysis attack mitigation technology
6.4 Electromagnetic analysis attack mitigation technology
7 Non-invasive attack test method
7.1 Overview
7.2 Test Strategy
7.3 Test Framework
7.4 Test process
7.5 Manufacturer Information Required for Testing

1 Foreword

GM/T 0083-2020 was issued by State Administration of Cryptography on 28 December 2020 and has been in force since 1 July 2021.

The GM/T prefix marks a recommended standard. It is not law in itself: it becomes binding when a contract names it, when a regulation or a mandatory standard refers to it, or when a producer declares conformity with it.

The document runs to 19 pages in English translation.

Preview: page 2 of 4 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0083-2020

2 Scope Preview

GM/T 0083-2020 - 2 Normative references 1 3 Terms and definitions 1 4 Symbols and abbreviations 2 4.1 Symbol 2 4.2 Abbreviations 3 5 Non-invasive attack methods 3 5.1 Overview 3 5.2 Naming and Classification 4 5.3 Analysis Process 4 5.4 Relevance to safety functions 5 6 Non-invasive attack mitigation techniques 6 6.1 Overview 6 6.2 Timing analysis attack mitigation technology 7 6.3 Energy analysis attack mitigation technology 7 6.4 Electromagnetic analysis attack mitigation technology 10 7 Non-invasive attack test method 11 7.1 Overview 11 7.2 Test Strategy 11 7.3 Test Framework 11 7.4 Test process 12

GM/T 0083-2020 falls under ICS 35.040, in the field of information technology.

This catalogue holds 105 other GM/T standards in that field.

In this catalogue, GM/T standards carry edition years from 2012 to 2024.

3 About this standard

Issued by: State Administration of Cryptography

English translation: about 19 pages

Chinese original: about 22,224 characters

4 Related standards

Standards on related subjects:

GM/T 0084-2020 - Guideline for the mitigation of physical attacks against cryptographic modules

GB/T 15843.1-2017 - Information technology -- Security techniques -- Entity authentication -- Part 1: General

GA/T 1389-2017 - Information Security Technology - Guidelines for Grading of Classified Protection of Cyber Security

GM/T 0080-2020 - SM9 cryptographic algorithm application specification

GM/T 0079-2020 - Direct anonymous attestation specification for trusted computing platform

GM/T 0078-2020 - The design guidelines for cryptographic random number generation module

Preview: page 3 of 4 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0083-2020

Chinastandards.org

5 Classification and status

International classification (ICS): 35.040

Chinese Standard Classification (CCS): L 80

Prefix GM/T: recommended standard.

Preview: page 4 of 4 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0083-2020