

ICS 35.040
CCS L 80

GM

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

GM/T 0084-2020

**Guideline for the mitigation of physical attacks against
cryptographic modules**

密码模块物理攻击缓解技术指南

(English Translation)

Issued on: December 28, 2020

Implemented on: July 1, 2021

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative References	2
Terms and Definitions	3
Data Imprinting Attack	4
Physical Attacks	5
Overview	6
Tamper-proofing	7
Tamper Resistance	8
Tamper Detection	9
Tamper Response	10
Tamper with Traces.....	11
Volume and weight	12
Mechanism of mixing and layering	13
Overview	14
Manual material removal	15
Mechanical processing	16
Waterjet processing	17
Laser processing	18
Chemical processing	19
Sandblasting	20
Energy-converged Cutting Technique.....	21
Overview	22
Radiation data imprinting attack	23
Temperature data imprinting attack.....	24
High voltage data imprinting attack	25
Abnormal high and low voltage	26
Equipment external encapsulation failure attack	27
Overview	28
Overview	29
Hard shell	30
Conformal coating	31
Insulating substrate	32

Special semiconductor topology	33
Opaque	34
Overview	35
Disposable photosensitive material	36
Gas analysis	37
Dose sensor	38
RFID polling	39
Voltage sensor	40
Probe sensor	41

1 Scope

This Standard specifies the physical security mechanism of cryptographic modules, physical attack methods, mitigation techniques used to prevent or detect these attacks, as well as mitigation measures at different stages of the life cycle, such as:

development, distribution and operation, etc.

This Standard is applicable to the guidance for the implementation of physical attack mitigation techniques in cryptographic modules and the verification of the tested cryptographic modules to achieve the most essential security assurance.

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.

GB/T 25069 Information Security Technology - Glossary GB/T 37092 Information Security Technology - Security Requirements for Cryptographic Modules

3 Terms and Definitions

What is defined in GB/T 37092, and the following terms and definitions are applicable to this document.

3.1 Data Imprinting Attack

Data imprinting attack refers means to take measures (such as: radiation and high temperature, etc.) to solidify the data in the memory circuit or the equipment containing

sensitive information, so that the data cannot be written-in or modified for a certain time.

3.2 Physical Attacks

Physical attacks refer to attacks that cause physical modification or abnormal operation restricts or prevents unauthorized physical access to computing systems by virtue of facilities, such as: guards, cameras, fences and buildings, etc.

The effectiveness of physical security satisfies the following conditions: when an attack is encountered, during the beginning of the attack or the subsequent penetration and destruction, the probability of the attack's success shall be extremely low, and the probability of detecting the attack shall be extremely high.

Physical security mechanism refers to the defensive measure used to protect sensitive data when encountering unauthorized physical access. It includes the utmost difficult to make unauthorized physical access to data (tamper resistance), the possession of a trigger mechanism used to prevent attacks (tamper detection) and the capability of saving traces of an attack attempt and finding previous attack attempts (tamper with traces) in the subsequent detections, etc.

For the cryptographic modules, physical attack refers to an attack that causes physical modification or abnormal operation of the cryptographic modules and performs unauthorized physical access to the cryptographic modules. The mitigation of physical attack refers to the defensive measure used to hinder or mitigate the physical attack.

The cryptographic modules not only have physical security threats when in use, but also may be subject to physical attacks at different stages of the life cycle, such as:

development, distribution and operation. Thus, the cryptographic modules shall have the capability of mitigating physical attacks during the development and distribution stages.

6.1 Overview

The physical security mechanism shall be applicable to different technical implementations, application environments and attack scenarios. Commonly seen physical security mechanisms include physical security mechanisms listed in 6.2 ~ 6.7 and physical security factors that may affect system security.

6.2 Tamper-proofing

Tamper-proofing refers to a physical security mechanism that can resist all known attacks and possible sudden attacks.

6.3 Tamper Resistance

Tamper resistance refers to the capability of providing protective measures to prevent physical security attacks and unauthorized physical access to data. For cryptographic modules that only have tamper resistance, only when tampering occurs does the owner of the cryptographic modules become aware of the occurrence of the tampering.

6.4 Tamper Detection

Tamper detection refers to the cryptographic modules' automatic determination of the behavior that attempts to destroy the physical security. After the cryptographic modules detect the intrusion behavior, they shall immediately and automatically respond.

6.5 Tamper Response

Tamper response refers to the action automatically taken by the cryptographic modules when the behavior that attempts to destroy the physical security of the cryptographic modules is detected. For cryptographic modules that rely on external responses, the operation of alarm may be adopted. For cryptographic modules that cannot rely on external responses, the operation of erasing or destroying secret data may be adopted.

6.6 Tamper with Traces

Tamper with traces can ensure that after the tampering occurs, the evidence left by the tampering will be retained by the cryptographic modules. This mechanism is achieved by chemistry or a combination of chemistry and mechanics. There shall be a long-term effective audit strategy in the cryptographic modules.

6.7.1 Volume and weight

When realizing the physical security mechanism, the influence of volume and weight shall be considered in combination with the practical application, so as to increase the difficulty of attack.

6.7.2 Mechanism of mixing and layering

Multiple layers and multiple types of physical security mechanism may be adopted to increase the difficulty of attack. Commonly seen hybrid mechanisms include (but are not limited to) the combination of tamper response and tamper resistance, and the deployment of the mechanism of tamper with traces at the periphery of the tamper resistance or tamper response mechanism.

---Combination of tamper response and tamper resistance. If the attacker enhances the techniques and can destroy the cryptographic modules with tamper resistance, the cryptographic modules shall be able to respond and reset the internal sensitive security