GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
RECORD NO.: 38306-2013

GM/T 0008-2012

Cryptography test criteria for security IC

安全芯片密码检测准则

Issued on: November 22, 2012 **Implemented on: November 22, 2012**

Issued by: State Cryptography Administration

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuer of this document shall not be held responsible for identifying any or all such patent rights.

This Standard was proposed by and shall be under the jurisdiction of the State Cryptography Administration.

The drafting organizations of this Standard: Commercial Cryptography Testing Centre of State Cryptography Administration, State Key Laboratory of Information Security, Tsinghua University, Beijing Hongsi Electronic Technologies Co., Ltd., Nationz Technologies Co., Ltd., Beijing CEC Huada Electronic Design Co., Ltd., Zhejiang University, Shenzhen Institutes of Advanced Technology of Chinese Academy of Sciences, Datang Microelectronics Co., Ltd., Beijing Xinguang-Tiandi IC Design Co., Ltd., Chengdu University of Information Technology.

The main drafters of this Standard: Li Dawei, Zhou Yongbin, Luo Peng, Liu Jiye, Zhang Jianren, Zhang Wenjing, Zhang Yiwei, Chen Lizhi, Ye Yin, Shen Haibin, Li Huiyun, Sun Dongyu, Xiong Yanping, Liu Hongwei, Chen Yun, Wu Zhen, Mao Yingying.

Cryptography test criteria for security IC

1 Scope

This Standard specifies three security levels of security capabilities which increase in sequence and the cryptographic test requirements which are applicable to the security chips of all security levels.

This Standard applies to both the cryptographic test of security chips and the development of security chips.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition dated applies to this document. For undated references, the latest edition of the referenced documents (including all amendments) applies to This Standard.

GM/T 0005, *Randomness test specification*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1

key

Key information or parameters which control cryptographic transformation operation.

3.1.2

sensitive information

Data in security chips which requires protection, except keys.

3.1.3

security chip

Integrated circuit chips which contain cryptographic algorithms and security functions and can implement key management mechanisms.

3.1.4

security capability

Direct or indirect assurance and protective measures which are provided by security chips for keys and sensitive information.

3.1.5

block cipher operation mode

The operation mode of block cipher algorithm, mainly including electronic code book mode (ECB), cipher block chaining mode (CBC), cipher feedback mode (CFB), output feedback mode (OFB), counter mode (CTR), etc.

3.1.6 public key cipher application mode

The application mode of public key cipher algorithm, mainly including encryption/decryption, signature/verification, key agreement, etc.

3.1.7

operation speed of cryptographic algorithm

Maximum data size that security chips can process within the unit time of cryptographic algorithm implementation.

3.1.8

physical random source

Source blocks of random sequences which is generated by the uncertainty of physical noise.

3.1.9

firmware

Procedure codes which is solidified in security chips, controlling and coordinating the cryptography and security functions of security chips.

3.1.10

hardware

such scenarios, security chips shall have basic protective capabilities for all kinds of security risks.

4.3 Security level 3

Security level 3 specifies the high security level requirements that the security capabilities of security chips can meet. Based on security level 2, security level 3 specifies the logical and/or physical protective measures that security chips shall have. Security level 3 requires security chips to provide high protection for keys and sensitive information; requires them to have the logical and/or physical security mechanism which is capable of providing complete protection for keys and sensitive information; requires them to be capable of defending all attacks specified in this Standard; requires test applicants to be capable of proving the effectiveness of relevant protective measures; and requires them to have complete life cycle assurances.

Security chips of security level 3 can be applied in the application scenarios in which the external operating environment for their deployment is incapable of ensuring their physical safety and the safety of input and output information. In such scenarios, security chips shall have comprehensive protective capabilities for all kinds of security risks.

5 Cryptographic algorithm

5.1 Random number generator

5.1.1 Security level 1

a) Security chips shall have at least 2 physical random sources independent to each other, which directly generate random numbers or the initial input of random number extension algorithm. The random numbers directly generated by or the initial input of random number extension algorithm generated by physical random sources shall be generated through exclusive-OR operation of all the output of physical random sources.

b) Within the operating conditions of temperature which are supported by security chips, set three operating conditions including temperature upper limit, temperature lower limit and room temperature, and the random numbers generated by security chips shall meet the randomness test requirements specified in GM/T 0005.

5.1.2 Security level 2

a) Security chips shall have at least 4 physical random sources independent to each other, which directly generate random numbers or the initial input of random number extension algorithm. The random numbers directly

Based on security level 2:

a) The stream cipher algorithms supported by security chips shall be implemented using special hardware circuits.

b) Security chips themselves can determine the correctness of the stream cipher algorithms supported by them.

6 Security chip interface

6.1 Physical interface

6.1.1 Security level 1

a) The physical interfaces supported by security chips shall not contain covert channels.

b) The operation data shall be consistent, which is input and output by different physical interfaces supported by security chips.

c) If security chips support the random number generation function, all the random numbers output by the physical interfaces supported by security chips are capable of passing the randomness test.

6.1.2 Security level 2

Based on security level 1, security chips shall not contain any physical interface except the physical interfaces declared.

6.1.3 Security level 3

Based on security level 2:

a) Security chips shall support shutting down the physical interfaces in the non-operating status.

b) Security chips shall not contain the physical interfaces of the security mechanism which is defined by possible side-channel security chips.

6.2 Logical interface

6.2.1 Security level 1

a) The logical interfaces supported by security chips shall not contain covert channels.

b) The operation data of the cryptographic algorithm shall be consistent,

b) Security chips shall support exporting keys in the form of ciphertexts.

7.6.3 Security level 3

As security level 2.

7.7 Clearing

7.7.1 Security level 1

Security chips are capable of clearing the stored keys correctly and effectively.

7.7.2 Security level 2

Based on security level 1:

a) The clearing of keys requires corresponding authorization.

b) The clearing of keys shall not disclose keys and key related information.

7.7.3 Security level 3

Based on security level 2, security chips shall support the secure key clearing mechanism which is implemented using the methods including repeated erasing.

8 Sensitive information protection

8.1 Storage

8.1.1 Security level 1

Security chips are capable of storing sensitive information correctly and effectively.

8.1.2 Security level 2

Based on security level 1:

a) Security chips shall support the storage of sensitive information in the form of ciphertexts.

b) Security chips shall have an access control mechanism for sensitive information.

8.1.3 Security level 3

Based on security level 2:

Based on security level 2, the operation of sensitive information shall be conducted in a controllable and special secure storage region.

8.4 Transmission

8.4.1 Security level 1

Security chips shall be capable of importing or exporting sensitive information permissible for transmission correctly and effectively, as needed.

8.4.2 Security level 2

Based on security level 1:

a) The transmission of sensitive information requires corresponding authorization.

b) The sensitive information permissible for transmission shall be transmitted in the form of ciphertexts.

c) For the sensitive information impermissible for transmission, security chips shall have a corresponding security mechanism to ensure sensitive information is only handled inside security chips.

8.4.3 Security level 3

As security level 2.

9 Firmware security

9.1 Storage

9.1.1 Security level 1

The firmware in security chips shall not be read out through interfaces.

9.1.2 Security level 2

Based on security level 1:

a) Except firmware itself, other codes shall not read-write the codes of firmware.

b) Except firmware itself, the reading-writing of the data in firmware by other codes requires corresponding authorization.

9.1.3 Security level 3

Based on security level 2:

a) Security chips shall have a shielding layer for active protection.

b) All logical circuits designed by themselves on the layout of security chips shall be wired together.

12.2 Self-destruction of keys and sensitive information

12.2.1 Security level 1

No requirement.

12.2.2 Security level 2

When security chips receive an external command for authorized self-destruction, they are capable of conducting the self-destruction of keys and sensitive information effectively and reliably.

12.2.3 Security level 3

Based on security level 2, security chips shall have an active capability of the self-destruction of keys and sensitive information.

12.3 Timing attack protection

12.3.1 Security level 1

No requirement.

12.3.2 Security level 2

a) Security chips shall have corresponding protective measures to ensure that there is no obvious correlation between the operation time and the keys and sensitive information, when operation is conducted for all cryptographic algorithms supported by security chips.

b) Test applicants shall use documentation or other methods to give descriptions and explanations for the corresponding protective measures and their effectiveness.

c) The effectiveness of protective measures shall pass the test.

12.3.3 Security level 3

Based on security level 2, test applicants shall use documentation or other methods to give proof for the corresponding protective measures and their effectiveness.

12.6 Protection to fault attack

12.6.1 Security level 1

No requirement.

12.6.2 Security level 2

a) When the changes of operating parameters which make security chips in a vulnerable status, including the voltage, frequency, temperature, etc. of the operating conditions of security chips, they shall be capable of finding the changes of these operating conditions, and take corresponding protective measures to protect keys and sensitive information from being disclosed.

b) Test applicants shall use documentation or other methods to give descriptions and explanations for the corresponding protective measures and their effectiveness.

c) The effectiveness of protective measures shall pass the test.

12.6.3 Security level 3

Based on security level 2:

a) Security chips shall have the resistivity to light attacks and take corresponding measures to protect keys and sensitive information from being disclosed.

b) Test applicants shall use documentation or other methods to give descriptions and explanations for the corresponding protective measures and their effectiveness.

13 Life cycle assurance

13.1 Organization qualifications

13.1.1 Security level 1

Have the qualifications which are recognized by the State Cryptography Administration.

13.1.2 Security level 2

As security level 1.

13.1.3 Security level 3

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------