ICS 35.040
L 80
备案号：38306—2013

GM

中华人民共和国密码行业标准

GM/T 0008—2012

安全芯片密码检测准则

Cryptography test criteria for security IC

2012-11-22 发布　　2012-11-22 实施

国家密码管理局　　发布

目　　次

前　言

本标准依据 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由国家密码管理局提出并归口。

本标准的主要起草单位：国家密码管理局商用密码检测中心、信息安全国家重点实验室、清华大学、北京宏思电子技术有限责任公司、国民技术股份有限公司、北京中电华大电子设计有限责任公司、浙江大学、中国科学院深圳先进技术研究院、大唐微电子技术有限公司、北京芯光天地集成电路设计有限公司、成都信息工程学院。

本标准的主要起草人：李大为、周永彬、罗鹏、刘继业、张建人、张文婧、张翌维、陈立志、叶茵、沈海斌、李慧云、孙东昱、熊燕萍、刘宏伟、陈运、吴震、毛颖颖。

引　言

安全芯片是一种重要的基础安全功能单元，在计算机、信息与通信系统中应用非常广泛。特别地，多数安全芯片都具有一种或多种密码功能。本标准中的安全芯片是指实现了一种或多种密码算法，直接或间接地使用密码技术来保护密钥和敏感信息的集成电路芯片。

安全芯片在实现的密码算法的基础上，根据设计和应用的不同须具有一种或多种安全能力。本标准将安全能力划分为密码算法、安全芯片接口、密钥管理、敏感信息保护、安全芯片固件安全、自检、审计、攻击的削弱与防护和生命周期保证九个部分，对每个部分的安全能力划分为安全性依次递增的三个安全等级，并对每个安全等级提出了安全性要求。安全芯片的安全等级定为该安全芯片所具有的各部分的安全能力的最低安全等级。

使用安全芯片所具有的密码功能时，安全芯片的安全能力对于保障整个系统的安全性举足轻重。为提供预期的安全服务，以及满足应用与环境的安全要求，应选择恰当安全等级的安全芯片，以确保使用安全芯片的计算机、信息与通信系统能够为特定应用提供一种可接受的安全等级。

本标准可以为选择满足应用与环境安全要求的适用安全等级的安全芯片提供依据，亦可为安全芯片的研制提供指导。

安全芯片密码检测准则

1 范围

本标准规定了安全能力依次递增的三个安全等级，以及适用于各安全等级安全芯片的密码检测要求。

本标准适用于安全芯片的密码检测，亦可指导安全芯片的研制。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GM/T 0005 随机性检测规范

3 术语、定义和缩略语

3.1 术语和定义

下列术语、定义适用于本文件。

3.1.1

密钥 key

控制密码变换操作的关键信息或参数。

3.1.2

敏感信息 sensitive information

安全芯片中除密钥外需要保护的数据。

3.1.3

安全芯片 security chip

含有密码算法、安全功能，可实现密钥管理机制的集成电路芯片。

3.1.4

安全能力 security capability

安全芯片对密钥和敏感信息能够提供的直接或间接的保障和防护措施。

3.1.5

分组密码算法的工作模式 block cipher operation mode

分组密码算法的工作方式，主要包括电码本模式(ECB)、密码分组链接模式(CBC)、密码反馈模式(CFB)、输出反馈模式(OFB)、计数器模式(CTR)等。

3.1.6

公钥密码算法的应用模式 public key cipher application mode

公钥密码算法的使用方式，主要包括加密/解密、签名/验证和密钥协商等。

3.1.7

密码算法的运算速率 operation speed of cryptographic algorithm

安全芯片实现的密码算法单位时间内可处理的最大数据量。