ICS 35.040
L 80
备案号:49740—2015

GM

中华人民共和国密码行业标准

GM/T 0041—2015

智能 IC 卡密码检测规范

Cryptographic test specification for smart card

2015-04-01 发布　　2015-04-01 实施

国家密码管理局　　发布

目　　次

前　言

本标准按照 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。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：北京华大智宝电子系统有限公司、国家密码管理局商用密码检测中心、武汉天喻信息产业股份有限公司、东信和平智能卡股份有限公司、北京握奇数据系统有限公司、航天信息股份有限公司、北京中电华大电子设计有限责任公司、上海华虹集成电路有限责任公司。

本标准主要起草人：陈跃、陈保儒、李大为、邓开勇、罗鹏、雷银花、林春、刘文娟、李晓俊、张汉就、刘蕾、罗世新、王晓燕、梁少峰。

智能 IC 卡密码检测规范

1 范围

本标准规定了智能 IC 卡产品的检测项目及检测方法。

本标准适用于智能 IC 卡产品的密码检测，也可用于指导智能 IC 卡产品的研发。智能 IC 卡产品包括但不限于金融 IC 卡、公交 IC 卡等。

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

GM/T 0039 密码模块安全检测要求

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 所界定的以及下列术语和定义适用于本文件。

3.1

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

3.2

非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥(公钥)可以公开，另一个密钥(私钥)必须保密，且由公钥求解私钥是计算不可行的。

3.3

密码杂凑算法 hash algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串，且满足下列 3 个特性：

a) 为一个给定的输出找出能映射到该输出的一个输入是计算上困难的；

b) 为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的；

c) 要发现不同的输入映射到同一输出是计算上困难的。

3.4

公钥 public key

非对称密码算法中可以公开的密钥。

3.5

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。