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

中华人民共和国密码
行业标准
智能IC卡密码检测规范
GM/T 0041—2015
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 28千字
2015年7月第一版 2015年7月第一次印刷
*
书号:155066·2-28770 定价 21.00 元

GM/T 0041-2015

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。

3.6

数字信封　digital envelope

一种数据结构，包含用对称密钥加密的密文和用公钥加密的该对称密钥。

3.7

测试对象　target of testing

本标准中测试对象专指智能IC卡。

4　符号和缩略语

下列符号和缩略语适用于本文件。

APDU　应用协议数据单元(Application Protocol Data Unit)

COS　芯片操作系统(Chip Operating System)

DDF　目录定义文件(Directory Definition File)

Lc　命令数据的长度(Length of Command Data)

MAC　报文鉴别代码(Message Authenticate Code)

PIN　个人识别号(Personal Indentify Number)

5　检测项目

5.1　COS安全管理功能检测

COS安全管理功能检测的目的是测试智能IC卡各项安全功能的运行情况，并检验实现的正确性。COS安全管理功能检测包括下列12个方面的测试：

a)　外部认证测试；

b)　内部认证测试；

c)　PIN认证测试；

d)　PIN修改测试；

e)　PIN重装测试；

f)　PIN解锁测试；

g)　应用锁定测试；

h)　应用解锁测试；

i)　非对称密钥密码算法公钥导入导出测试；

j)　非对称密钥密码算法解密私钥导入测试；

k)　非对称密钥密码算法产生数字信封测试；

l)　非对称密钥密码算法打开数字信封测试。

5.2　COS安全机制检测

COS的安全机制检测的目的是测试智能IC卡COS为了实现安全管理而采取的手段和方法的正确性及有效性。COS安全机制检测包括下列4个方面的测试：

a)　报文安全传送测试；

b)　密钥安全传送测试；

c)　安全状态和访问权限测试；

d)　应用防火墙测试。

5.3 密钥的素性检测

智能IC卡生成的RSA密钥的素性应满足大素数的要求。

5.4 随机数质量检测

智能IC卡生成的随机数的随机性应符合GM/T 0005中的要求。

5.5 密码算法实现正确性检测

密码算法实现正确性检测包括下列6个方面的测试：

a) 分组算法实现正确性测试；
b) 非对称密钥密码算法密钥生成正确性测试；
c) 非对称密钥密码算法加密解密实现正确性测试；
d) 非对称密钥密码算法数字签名及签名验证正确性测试；
e) 杂凑算法实现正确性测试；
f) 序列算法正确性测试。

5.6 密码算法实现性能检测

密码算法实现性能检测包括下列11个方面性能测试：

a) 分组密钥密码算法的加密性能测试；
b) 分组密钥密码算法的解密性能测试；
c) 杂凑算法性能测试；
d) 非对称密钥密码算法的加密性能测试；
e) 非对称密钥密码算法的解密性能测试；
f) 非对称密钥密码算法的数字签名性能测试；
g) 非对称密钥密码算法的签名验证性能测试；
h) 非对称密钥密码算法密钥对生成性能测试；
i) 序列算法加密性能测试；
j) 序列算法解密性能测试；
k) 序列算法完整性性能测试。

5.7 设备安全性测试

智能IC卡安全性测试项目遵照GM/T 0039。

6 检测方法

6.1 总体要求

如果送检产品有为测试独立开放的测试接口指令，需要在送检文档中加以明确说明，并在检测完毕后予以失效。

独立开放的测试接口只用于检测使用，不提供应用密码服务。

6.2 COS安全管理功能检测

6.2.1 外部认证测试

6.2.1.1 正常情况测试

测试步骤如下：

a) 正确的外部认证密钥进行认证，测试对象应返回认证成功的响应；
b) 在认证前操作需要安全状态的文件，测试对象应返回不满足安全状态；
c) 在认证后操作需要安全状态的文件，测试对象应返回操作成功。

6.2.1.2 异常情况测试

测试步骤如下：
a) 用错误的外部认证密钥去认证，测试对象应返回认证不成功并提示剩余认证次数，当剩余认证次数为零时，外部认证密钥锁定；
b) 用错误的外部认证密钥去认证，在认证后操作需要安全状态的文件，测试对象应返回不满足安全状态；
c) 用错误的密钥标识去做外部认证，测试对象应返回密钥没有找到；
d) 当测试对象存在多个外部认证密钥，成功认证外部认证密钥 1，操作受外部认证密钥 2 保护的文件，测试对象应返回不满足安全状态。

6.2.2 内部认证测试

使用标准测试数据进行内部认证，测试对象应返回的结果应与预期结果一致。

6.2.3 PIN 认证测试

6.2.3.1 正常情况测试

测试步骤如下：
a) 使用正确的 PIN 进行认证，测试对象应返回认证成功响应；
b) 在认证前操作需要 PIN 保护的文件，测试对象应返回不满足安全状态；
c) 在认证后操作需要 PIN 保护的文件，测试对象应返回操作成功。

6.2.3.2 异常情况测试

测试步骤如下：
a) 使用错误的 PIN 去认证，测试对象应返回认证不成功及剩余的认证次数，当剩余的认证次数为零时，PIN 锁定；
b) 使用错误的 PIN 去认证，剩余认证次数应该减一，在 PIN 锁定前，使用正确的 PIN 认证，剩余尝试次数应恢复为预定值；
c) 当测试对象支持多 PIN 时，成功认证 PIN1 后，操作受 PIN2 保护的文件，测试对象应返回不满足安全状态；
d) 使用错误的密钥标识去认证，测试对象应返回不成功；
e) 使用错误的 PIN 值去认证，在认证后操作需要 PIN 保护的文件，测试对象应返回不满足安全状态。

6.2.4 PIN 修改测试

6.2.4.1 正常情况测试

测试步骤如下：
a) 用与原 PIN 值不同的 PIN 进行修改，测试对象应返回修改成功；
b) 认证修改之前的 PIN，测试对象应返回认证失败；操作需要 PIN 保护的文件，测试对象应返回不满足安全状态；

c) 认证修改之后的 PIN，测试对象应返回认证成功；操作需要 PIN 保护的文件，测试对象应返回操作成功。

6.2.4.2 异常情况测试

测试步骤如下：

a) PIN 的长度超出规定范围，测试对象应返回数据参数错误；
b) 用错误的原 PIN 值进行修改，测试对象应返回修改不成功；
c) 用错误的原 PIN 值进行修改，达到最大尝试次数后，PIN 锁定；
d) PIN 锁定的情况下，使用正确的原 PIN 进行修改，应不成功。

6.2.5 PIN 重装测试

6.2.5.1 正常情况测试

测试步骤如下：

a) 用与原 PIN 值不同的 PIN 进行重装，测试对象应返回重装成功；
b) 认证重装之前的 PIN，测试对象应返回认证失败；操作需要 PIN 保护的文件，测试对象应返回不满足安全状态；
c) 认证重装之后的 PIN，测试对象应返回认证成功；操作需要 PIN 保护的文件，测试对象应返回操作成功。

6.2.5.2 异常情况测试

测试步骤如下：

a) 用错误的 Lc 计算 MAC 进行重装操作，测试对象应返回安全报文错误；
b) 用错误的填充方法计算 MAC 进行重装操作，测试对象应返回安全报文错误；
c) 用错误的密钥计算 MAC 进行重装操作，测试对象应返回安全报文错误；
d) 未取随机数直接计算 MAC 进行重装操作，测试对象应返回未取随机数；
e) PIN 的长度超出设计范围，测试对象应返回不成功；
f) 连续 3 次使用错误的密钥计算 MAC 进行重装操作，应用锁定；
g) PIN 锁定情况下，使用正确的密钥进行 PIN 重装，应不成功。

6.2.6 PIN 解锁测试

6.2.6.1 正常情况测试

测试步骤如下：

a) 多次认证错误的 PIN 使其锁定，用正确的方法计算 MAC 进行解锁，测试对象应返回解锁成功；
b) 未认证 PIN，操作需要 PIN 保护的文件，测试对象应返回不满足安全状态；
c) 认证解锁之后的 PIN，测试对象应返回认证成功；
d) 操作需要 PIN 保护的文件，测试对象应返回操作成功。

6.2.6.2 异常情况测试

测试步骤如下：

a) 用错误的 Lc 计算 MAC 进行解锁操作，测试对象应返回安全报文错误；
b) 用错误的填充方法计算 MAC 进行解锁操作，测试对象应返回安全报文错误；

c) 用错误的密钥计算 MAC 进行解锁操作，测试对象应返回安全报文错误；
d) 未取随机数直接计算 MAC 进行解锁操作，测试对象应返回未取随机数；
e) PIN 的长度超出设计范围，测试对象应返回不成功；
f) 连续 3 次使用错误的密钥计算 MAC 进行解锁操作，应用锁定。

6.2.7 应用锁定测试

6.2.7.1 正常情况测试

测试步骤如下：
a) 用正确的方法计算 MAC 进行应用锁定，测试对象应返回应用锁定成功；
b) 应用临时锁定后，仅可以执行选择应用、取响应数据、取随机数、应用解锁指令，否则，测试对象返回使用条件不满足；
c) 应用永久锁定后，仅可以执行选择应用、取响应数据、取随机数指令，否则，测试对象返回应用永久锁定。

6.2.7.2 异常情况测试

测试步骤如下：
a) 用错误的 Lc 计算 MAC 进行应用锁定操作，测试对象应返回安全报文错误；
b) 用错误的填充方法计算 MAC 进行应用锁定操作，测试对象应返回安全报文错误；
c) 用错误的密钥计算 MAC 进行应用锁定操作，测试对象应返回安全报文错误；
d) 未取随机数直接计算 MAC 进行应用锁定操作，测试对象应返回未取随机数；
e) 在 DDF 下使用应用锁定命令，测试对象应返回使用条件不满足；
f) 锁定一个应用，选择其他的应用应都不返回应用锁定。

6.2.8 应用解锁测试

6.2.8.1 正常情况测试

测试步骤如下：
a) 用正确的方法计算 MAC 进行应用解锁，测试对象应返回解锁成功；
b) 应用解锁后，可以执行除选择应用、取响应数据、取随机数、应用解锁指令之外的其他指令。

6.2.8.2 异常情况测试

测试步骤如下：
a) 用错误的 Lc 计算 MAC 进行应用解锁操作，测试对象应返回安全报文错误；
b) 用错误的填充方法计算 MAC 进行应用解锁操作，测试对象应返回安全报文错误；
c) 用错误的密钥计算 MAC 进行应用解锁操作，测试对象应返回安全报文错误；
d) 未取随机数直接计算 MAC 进行应用解锁操作，测试对象应返回未取随机数；
e) 在 DDF 下使用应用解锁命令，测试对象应返回使用条件不满足；
f) 解锁一个应用，选择其他被锁定的应用，应还处于锁定状态。

6.2.9 非对称密钥密码算法公钥导入导出测试

6.2.9.1 正常情况测试

测试步骤如下：

a） 导入测试：

1） 在测试对象外，使用指定的私钥对数据进行签名；

2） 将指定的公钥写入指定的公钥文件；

3） 测试对象使用该公钥对特定的签名结果进行签名验证运算，测试对象应能验证通过。

b） 导出测试：

1） 测试对象产生密钥对，导出公钥值；

2） 测试对象用私钥对特定数据进行签名运算；

3） 在测试对象外，使用该公钥对签名结果进行签名验证运算，应能验证通过。

6.2.9.2 异常情况测试

未生成密钥对，执行公钥导出指令，测试对象应返回不成功。

6.2.10 非对称密钥密码算法解密私钥导入测试

6.2.10.1 正常情况测试

指定密钥方式测试：

a） 将指定的私钥采用带 MAC 的密文方式写入指定的解密私钥文件；

b） 使用该私钥对特定数据进行解密运算，测试对象的计算结果应与预期结果一致。

6.2.10.2 异常情况测试

测试步骤如下：

a） 用错误的 Lc 计算 MAC 进行私钥写入操作，测试对象应返回安全报文错误；

b） 用错误的填充方法计算 MAC 进行私钥写入操作，测试对象应返回安全报文错误；

c） 用错误的密钥计算 MAC 进行私钥写入操作，测试对象应返回安全报文错误；

d） 未取随机数直接计算 MAC 进行私钥写入操作，测试对象应返回未取随机数。

6.2.11 非对称密钥密码算法产生数字信封测试

6.2.11.1 正常情况测试

指定密钥方式测试：

a） 将指定公钥写入指定的公钥文件；

b） 将会话密钥作为数据，使用该公钥产生数字信封，测试对象应返回信封数据；

c） 使用该会话密钥对明文数据进行加密运算，得到密文数据；

d） 在测试对象外部验证密文的正确性。

6.2.11.2 异常情况测试

用非公钥文件产生数字信封，测试对象应返回不成功。

6.2.12 非对称密钥密码算法打开数字信封测试

6.2.12.1 正常情况

产生密钥方式测试：

a） 产生一个非对称密钥对，将公钥导出；

b） 使用该公钥在测试对象外部产生数字信封，并使用会话密钥对明文数据进行加密，得到密文

数据；

c) 测试对象用私钥打开数字信封，得到会话密钥，并对密文数据进行解密运算，运算结果应与原明文数据一致。

6.2.12.2 异常情况

用非私钥文件打开数字信封，测试对象应返回不成功。

6.3 COS 安全机制检测

6.3.1 报文安全传送测试

6.3.1.1 正常情况测试

带 MAC 的密文方式测试：

a) 用带 MAC 的密文方式更新基本文件；
b) 用送入 MAC 的方式读出密文基本文件内容；
c) 检测机构将读出的密文进行解密；
d) 解密的数据应与写入的内容相一致；
e) 用不同的数据长度进行测试。

6.3.1.2 异常情况测试

测试步骤如下：

a) 用错误的 Lc 计算 MAC 进行读写操作，测试对象应返回安全报文错误；
b) 用错误的填充方法计算 MAC 进行读写操作，测试对象应返回安全报文错误；
c) 用错误的密钥计算 MAC 进行读写操作，测试对象应返回安全报文错误；
d) 未取随机数直接计算 MAC 进行读写操作，测试对象应返回未取随机数；
e) 用明文方式进行读写操作，测试对象应返回文件类型错；
f) 用密文方式进行读写操作，测试对象应返回文件类型错；
g) 连续 3 次使用错误的密钥计算 MAC 进行读写操作，应用锁定。

6.3.2 密钥安全传送测试

6.3.2.1 正常情况测试

测试步骤如下：

a) 用带 MAC 的密文方式写入外部认证密钥，并进行外部认证，测试对象应返回认证成功的响应；
b) 用带 MAC 的密文方式写入内部认证密钥，并进行内部认证，测试对象应返回认证成功的响应；
c) 用带 MAC 的密文方式写入 PIN，并进行 PIN 验证，测试对象应返回认证成功的响应；
d) 用带 MAC 的密文方式更新外部认证密钥；
e) 用未更新的外部认证密钥值进行外部认证，测试对象应返回认证不成功；
f) 用更新的外部认证密钥进行外部认证，测试对象应返回认证成功响应；
g) 用带 MAC 的密文方式更新内部认证密钥并进行内部认证，返回的结果应与预期结果一致。

6.3.2.2 异常情况测试

测试步骤如下：

a) 用错误的 Lc 计算 MAC 进行读写操作，测试对象应返回安全报文错误；
b) 用错误的填充方法计算 MAC 进行读写操作，测试对象应返回安全报文错误；
c) 用错误的密钥计算 MAC 进行读写操作，测试对象应返回安全报文错误；
d) 未取随机数直接计算 MAC 进行读写操作，测试对象应返回未取随机数；
e) 用错误的 Lc 加密数据进行读写操作，测试对象应返回安全报文数据项不正确；
f) 对要求用密文带 MAC 写的密钥用密文方式写，测试对象应返回文件类型错。

6.3.3 安全状态和访问权限测试

6.3.3.1 写文件权限测试

测试步骤如下：
a) 未获得权限，写文件，测试对象应返回不满足安全状态；
b) 获得权限后，写文件成功执行；
c) 重新选择文件目录，读取写入文件，确认写入文件内容正确。

6.3.3.2 读文件权限测试

测试步骤如下：
a) 未获得权限，读文件，测试对象应返回不满足安全状态；
b) 获得权限后，读文件成功执行。

6.3.3.3 写密钥权限测试

测试步骤如下：
a) 未获得权限，写密钥，测试对象应返回不满足安全状态；
b) 获得权限后，写密钥成功执行。

6.3.3.4 对称密钥使用权限测试

测试步骤如下：
a) 未获得权限，使用密钥，测试对象应返回不满足安全状态；
b) 获得权限后，密钥可以使用。

6.3.3.5 非对称密钥使用权限测试

测试步骤如下：
a) 未获得权限，使用非对称密钥，测试对象应返回不满足安全状态；
b) 获得权限后，可以成功使用非对称密钥运算。

6.3.4 应用防火墙测试

测试步骤如下：
a) 外部认证安全状态测试：
   1) 选择应用 1，认证外部认证密钥，获取相应权限，操作需要该权限的文件，测试对象应返回成功的响应；
   2) 选择应用 2，操作需要该权限的文件，测试对象应返回不满足安全状态；
   3) 返回应用 1，操作需要同样权限的文件，测试对象应返回不满足安全状态。
b) PIN 认证安全状态测试：

1） 选择应用1，正确进行PIN认证，获取文件的修改权限；
2） 选择应用2，再选择应用1，不进行PIN认证对此文件进行修改，应该返回不满足安全状态。

c） 应用锁定状态测试：
1） 锁定应用1；
2） 选择应用2，应可以正常操作。

d） 应用解锁状态测试：
1） 对其中一个已锁定的应用进行解锁操作，解锁成功后，该应用应能正常操作；
2） 操作其他已锁定的应用，应都返回不满足安全状态。

e） 文件更新测试：
1） 选择应用1，读出所有文件内容；
2） 选择应用2，更新其中一个文件；
3） 返回应用1，读出所有文件内容，其内容不变。

6.4 RSA密钥的素性检测

6.4.1 素数采集

使用“素数生成”命令，连续采集N对素数对。N不小于1 000。

6.4.2 数据分析

验证获取的素数对数据应满足素性要求。

6.5 随机数质量检测

对于具有随机数生成功能的智能IC卡，为确保随机数质量应进行此项测试。

6.5.1 随机数采集

使用“随机数生成”命令，连续采集N个随机数文件。N不小于1 000，单个文件不小于128 k字节。

6.5.2 数据分析

测试方法见GM/T 0005。

6.6 密码算法实现正确性检测

6.6.1 分组密码算法加密解密实现正确性测试

测试步骤如下：

a） 执行分组密码算法的运算指令，采用指定密钥进行运算；
b） 通过加密和解密运算，生成密文结果和还原明文数据；
c） 运算结果应能通过正确性验证。

6.6.2 非对称密钥密码算法加密解密实现正确性测试

测试步骤如下：

a） 执行非对称密钥加解密运算指令；
b） 通过加密和解密运算，生成密文结果和还原明文数据；

c) 运算结果应能通过正确性验证。

6.6.3 非对称密钥密码算法数字签名及签名验证实现正确性测试

测试步骤如下：

a) 执行非对称密钥密码算法的签名运算指令；

b) 导出公钥，对数据进行签名验证；

c) 使用测试密钥对数据进行卡外签名；

d) 将公钥导入到卡内，执行非对称密码算法的签名验证指令。

6.6.4 杂凑算法实现正确性测试

测试步骤如下：

a) 生成随机数据，使用 IC 卡进行杂凑算法运算，得到计算结果；

b) 运算结果应能通过正确性验证。

6.6.5 非对称密钥密码算法密钥生成正确性测试

测试步骤如下：

a) 生成非对称密钥对，应返回成功；

b) 使用非对称密钥对特定数据加密，应返回成功；

c) 使用非对称密钥对加密结果解密，应返回成功，运算结果应能通过正确性验证。

6.6.6 序列算法实现正确性测试

测试步骤如下：

a) 执行采用序列密码算法的运算指令，采用指定密钥进行运算；

b) 运算结果应能通过正确性验证。

6.7 密码算法实现性能检测

6.7.1 分组算法加密性能测试

测试步骤如下：

a) 使用随机数据，随机密钥，执行分组算法加密指令进行加密运算 1 000 次；

b) 验证加密结果正确性；

c) 累积总的运算时间 T；

d) 计算加密速率。

6.7.2 分组算法解密性能测试

测试步骤如下：

a) 使用随机数据，随机密钥，执行分组算法解密指令进行解密运算 1 000 次；

b) 验证解密结果正确性；

c) 累积总的运算时间 T；

d) 计算解密速率。

6.7.3 杂凑算法实现性能测试

测试步骤如下：

a) 变化数据长度，从 1 字节到 N 字节（$N>128$），执行杂凑算法指令进行运算；
b) 验证计算结果；
c) 累积总的运算时间 T；
d) 计算杂凑速率。

6.7.4 非对称密钥密码算法加密性能测试

测试步骤如下：
a) 使用测试密钥，使用随机数据，执行非对称算法加密指令进行运算 1 000 次；
b) 验证加密结果正确性；
c) 累积总的运算时间 T；
d) 计算加密速率。

6.7.5 非对称密钥密码算法解密性能测试

测试步骤如下：
a) 使用测试密钥，使用标准数据，执行非对称算法指令进行解密运算 1 000 次；
b) 验证结果正确性；
c) 累积总的运算时间 T；
d) 计算解密速率。

6.7.6 非对称密钥密码算法数字签名性能测试

测试步骤如下：
a) 使用测试密钥，使用随机数据，执行非对称算法签名指令进行运算 1 000 次；
b) 验证结果正确性；
c) 累积总的运算时间 T；
d) 计算签名速率。

6.7.7 非对称密钥密码算法签名验证性能测试

测试步骤如下：
a) 使用测试密钥，使用标准数据，执行非对称算法签名验证指令进行运算 1 000 次；
b) 验证结果正确性；
c) 累积总的运算时间 T；
d) 计算签名验证速率。

6.7.8 非对称密钥密码算法密钥对生成性能测试

测试步骤如下：
a) 连续生成非对称密钥对，执行 1 000 次操作；
b) 累计总的运算时间 T；
c) 计算密钥对生成性能。

6.7.9 序列算法加密性能测试

测试步骤如下：
a) 使用随机数据，随机密钥，执行序列算法指令进行加密运算 1 000 次；
b) 验证加密结果正确性；

c) 累积总的运算时间 T；
d) 计算加密速率。

6.7.10 序列算法解密性能测试

测试步骤如下：
a) 采用随机数据，随机密钥，通过序列算法指令进行解密运算 1 000 次；
b) 验证解密结果正确性；
c) 累积总的运算时间 T；
d) 计算解密速率。

6.7.11 序列算法完整性性能测试

测试步骤如下：
a) 采用随机数据，随机密钥，通过序列算法指令进行完整性运算 1 000 次；
b) 验证解密结果正确性；
c) 累积总的运算时间 T；
d) 计算解密速率。

6.8 设备安全性测试

智能 IC 卡安全性测试方法遵照 GM/T 0039。

7 合格性判定准则

测试对象符合下列条件，可判定为合格：
a) 至少使用一种经国家密码管理主管部门批准的密码算法；
b) 应通过 6.2 规定的全部或部分测试：
   1) 如测试对象支持外部认证命令，应通过 6.2.1 规定的测试；
   2) 如测试对象支持内部认证命令，应通过 6.2.2 规定的测试；
   3) 如测试对象支持 PIN 认证命令，应通过 6.2.3 规定的测试；
   4) 如测试对象支持 PIN 修改命令，应通过 6.2.3 和 6.2.4 规定的测试；
   5) 如测试对象支持 PIN 重装命令，应通过 6.2.3 和 6.2.5 规定的测试；
   6) 如测试对象支持 PIN 解锁命令，应通过 6.2.3 和 6.2.6 规定的测试。
c) 应通过 6.3 规定的全部或部分测试：
   1) 应通过 6.3.1 规定的测试；
   2) 应通过 6.3.2 规定的测试；
   3) 应通过 6.3.3 规定的测试；
   4) 如测试对象支持多应用，应通过 6.3.4 规定的测试。
d) 如测试对象具有 RSA 算法密钥对生成功能，应通过 6.4 规定的测试；
e) 应通过 6.5 规定的测试；
f) 应通过 6.6 规定的全部或部分测试：
   1) 如测试对象支持分组密码算法，应通过 6.6.1 规定的测试；
   2) 如测试对象支持非对称密钥密码算法，应通过 6.6.2 和 6.6.3 规定的测试；
   3) 如测试对象支持杂凑算法，应通过 6.6.4 规定的测试；
   4) 如测试对象支持序列算法，应通过 6.6.6 规定的测试。
g) 如测试对象具有单独的密码算法指令，应通过 6.7 规定的测试。

参 考 文 献

[1] GB/T 16649—2006 识别卡 带触点的集成电路卡
[2] GM/T 0002—2012 SM4 分组密码算法
[3] GM/T 0004—2012 SM3 密码杂凑算法
[4] GM/T 0009—2012 SM2 密码算法使用规范
[5] GM/T 0010—2012 SM2 密码算法加密签名消息语法规范
[6] GM/T 0028—2014 密码模块安全技术要求