ICS 35.030
CCS L 80

中华人民共和国密码行业标准

GM/T 0041—2024
代替 GM/T 0041—2015

智能 IC 卡密码检测规范

Cryptographic test specification for smart card

2024-12-27 发布　　2025-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GM/T 0041—2015《智能IC卡密码检测规范》，与GM/T 0041—2015相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了“检测环境”一章（见第5章）；

b) 更改了内部认证测试要求，增加了标准测试数据的含义和测试步骤（见7.2.2，2015年版的6.2.2）；

c) 更改了非对称密钥使用权限测试方法，增加了私钥使用权限的测试步骤（见7.3.3.5，2015年版的6.3.3.5）；

d) 更改了素数采集要求，增加了单组数据的数据量大小要求（见7.4.1，2015年版的6.4.1）；

e) 更改了随机数采集要求，增加了对于三级密码模块产品大数据量采集测试要求（见7.5.1，2015年版的6.5.1）；

f) 更改了非对称密码算法实现正确性的验证方法（见7.6.2，2015年版的6.6.2）；

g) 更改了非对称密码算法密钥生成的正确性测试方法，增加了测试次数和配对一致性检测步骤，并将配对一致性检测列为单独的测试项（见7.6.6，2015年版的6.6.5）；

h) 增加了“送检技术文档要求”一章（见第8章）。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京华大智宝电子系统有限公司、商用密码检测认证中心、武汉天喻信息产业股份有限公司、东信和平科技股份有限公司、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。

本文件主要起草人：陈跃、陈保儒、王雪聪、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、费林深。

本文件及其所代替文件的历次版本发布情况为：

——2015年首次发布为GM/T 0041—2015；

——本次为第一次修订。

智能 IC 卡密码检测规范

1 范围

本文件规定了智能 IC 卡产品的检测项目、检测方法、送检技术文档要求和判定规则。

本文件适用于智能 IC 卡产品的密码检测，也用于指导智能 IC 卡产品的研发。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 随机数检测规范

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 界定的术语和定义适用于本文件。

注：本文件中测试对象指智能 IC 卡。

4 缩略语

下列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）

IC：集成电路（Integrated Circuit）

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）

RSA：非对称密码算法（Rivest-Shamir-Adleman Algorithm）

5 检测环境

5.1 检测环境拓扑图

智能 IC 卡密码检测环境参考拓扑图如图 1 所示。

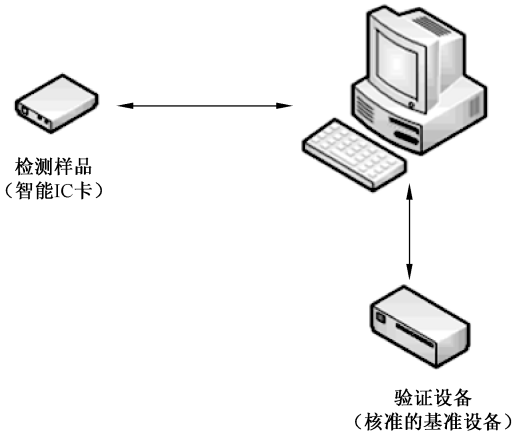

图 1　智能 IC 卡密码检测环境参考拓扑图

5.2　检测仪器

检测仪器见表 1。

表 1　检测仪器列表

仪器名称	备注
检测用 PC	用于运行操作系统及检测软件
核准的基准设备	用于密码算法的基准运算，作为验证用的智能 IC 卡密码或其他设备

5.3　检测软件

检测软件见表 2。

表 2　检测软件列表

软件名称	备注
检测平台软件	用于执行检测的软件工具
操作系统	用于运行检测平台软件的操作系统

6　检测项目

6.1　COS 安全管理功能检测

应包括下列 12 个方面的全部或部分测试：

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） 公钥导入导出测试；
j） 私钥导入测试；
k） 数字信封产生测试；
l） 数字信封打开测试。

6.2 COS 安全机制检测

应包括下列 3 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。
如测试对象支持多应用，还应包括：
d） 应用防火墙测试。

6.3 密钥的素性检测

应检测智能 IC 卡生成的 RSA 密钥的素性。

6.4 随机数质量检测

应检测智能 IC 卡生成的随机数质量。

6.5 密码算法实现正确性检测

应包括下列 6 个方面的测试，其中 a)～e)为必测项：
a） 分组密码算法加密解密实现正确性测试；
b） 非对称密码算法密钥生成正确性和配对一致性测试；
c） 非对称密码算法加密解密实现正确性测试；
d） 非对称密码算法数字签名与签名验证实现正确性测试；
e） 杂凑密码算法实现正确性测试；
f） 序列密码算法实现正确性测试。

6.6 密码算法实现性能检测

应包括下列 11 方面的测试，其中 a)～h)为必测项：
a） 分组密码算法加密性能测试；
b） 分组密码算法解密性能测试；
c） 非对称密码算法密钥对生成性能测试；
d） 非对称密码算法加密性能测试；
e） 非对称密码算法解密性能测试；
f） 非对称密码算法数字签名性能测试；
g） 非对称密码算法签名验证性能测试；
h） 杂凑密码算法实现性能测试；
i） 序列密码算法加密性能测试；
j） 序列密码算法解密性能测试；
k） 序列密码算法完整性性能测试。

6.7 设备安全性测试

智能 IC 卡安全性测试项目应遵照 GM/T 0039。

7 检测方法

7.1 总体要求

所有与智能 IC 卡之间的命令和响应交互均通过 APDU 实现。

7.2 COS 安全管理功能检测

7.2.1 外部认证测试

7.2.1.1 正常情况测试

测试步骤如下：

a) 使用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状态；

b) 在认证后操作（如增、删、改、查，下同）需要安全状态的文件，测试对象应返回操作成功。

7.2.1.2 异常情况测试

测试步骤如下：

a) 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；

b) 用错误的外部认证密钥进行认证，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；

c) 用错误的外部认证密钥进行认证，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；

d) 用错误的密钥标识进行做外部认证，测试对象应返回不成功；

e) 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。

7.2.2 内部认证测试

使用标准测试数据进行内部认证，测试对象返回的结果应与预期结果一致。标准测试数据是指预置的与内部认证用相同算法和密钥的输入和加密结果数据。

测试步骤如下：

a) 使用标准测试数据，执行内部认证指令；

b) 用内部认证密钥进行加密，返回加密结果；

c) 将返回结果与预期结果进行一致性比较，若一致，则通过。

7.2.3 PIN 认证测试

7.2.3.1 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状态；

b) 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。

7.2.3.2 异常情况测试

测试步骤如下：

a) 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；
b) 使用错误的 PIN 进行认证，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；
c) 使用错误的 PIN 进行认证，剩余认证次数应减一，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；
d) 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；
e) 使用错误的密钥标识进行认证，测试对象应返回不成功；
f) 使用错误的 PIN 进行认证，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。

7.2.4 PIN 修改测试

7.2.4.1 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) 用修改前的 PIN 进行认证，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) 用修改后的 PIN 进行认证，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。

7.2.4.2 异常情况测试

测试步骤如下：

a) 输入的 PIN 长度超出产品声称的范围，测试对象应返回数据参数错误；
b) 用错误的原 PIN 值调用 PIN 修改指令，测试对象应返回修改不成功；
c) 用错误的原 PIN 值调用 PIN 修改指令，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。

7.2.5 PIN 重装测试

7.2.5.1 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。

7.2.5.2 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) 按产品声称的次数连续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。

7.2.6 PIN 解锁测试

7.2.6.1 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。

7.2.6.2 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) 按产品声称的次数连续使用错误的密钥计算 MAC 进行解锁操作，应用锁定。

7.2.7 应用锁定测试

7.2.7.1 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。

7.2.7.2 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。

7.2.8 应用解锁测试

7.2.8.1 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。

7.2.8.2 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。

7.2.9 公钥导入导出测试

7.2.9.1 正常情况测试

测试步骤如下：

a) 导入测试

1) 调用基准卡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。

7.2.9.2 异常情况测试

在未生成密钥对的情况下，执行公钥导出指令，测试对象应返回不成功。

7.2.10 私钥导入测试

7.2.10.1 正常情况测试

指定密钥方式测试，测试步骤如下：

a) 将指定的私钥用带 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。

7.2.10.2 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。

7.2.11 产生数字信封测试

7.2.11.1 正常情况测试

指定密钥方式测试，测试步骤如下：
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。

7.2.11.2 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。

7.2.12 打开数字信封测试

7.2.12.1 正常情况测试

产生密钥方式测试，测试步骤如下：
a) 产生一个公私钥对，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。

7.2.12.2 异常情况测试

用非私钥文件打开数字信封，测试对象应返回不成功。

7.3 COS 安全机制检测

7.3.1 报文安全传送测试

7.3.1.1 正常情况测试

用密文＋MAC 模式测试，测试步骤如下：
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) 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。测试数据的长度宜取值：16 字节、32 字节、256 字节，或送检单位建议的长度。

7.3.1.2 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) 按产品声称的次数连续使用错误的密钥计算 MAC 进行读写操作，应用锁定。

7.3.2 密钥安全传送测试

7.3.2.1 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状态；
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状态；
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状态；
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状态；
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。

7.3.2.2 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。

7.3.3 安全状态和访问权限测试

7.3.3.1 写文件权限测试

测试步骤如下：

a) 在未获得权限情况下，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。

7.3.3.2 读文件权限测试

测试步骤如下：

a) 在未获得权限情况下，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。

7.3.3.3 写密钥权限测试

测试步骤如下：

a) 在未获得权限情况下,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。

7.3.3.4 对称密钥使用权限测试

测试步骤如下:
a) 在未获得权限情况下,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。

7.3.3.5 非对称密钥使用权限测试

测试步骤如下:
a) 在未获得权限情况下,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;
c) 不应有输出明文私钥的指令;
d) 私钥删除后不能再使用。

7.3.3.6 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状态;
   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。

7.4 RSA 密钥的素性检测

7.4.1 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。

每对素数中的单个素数长度应符合 GM/T 0005 和 GM/T 0039 的要求,具体为每个素数的长度应不低于 2 048 位。

7.4.2 数据分析

验证获取的素数对数据是否满足 GM/T 0005 中的素性要求。

7.5 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。

7.5.1 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，单个文件的数据量应不小于 128 KB。

对于三级密码模块产品，还应进行大数据量采集测试，具体为每个文件的数据量应不小于 1 GB，以确保其在高负载下的随机数质量。

7.5.2 数据分析

测试方法见 GM/T 0005。

7.6 密码算法实现正确性检测

7.6.1 分组密码算法加密解密实现正确性测试

测试步骤如下：

a) 执行分组密码算法运算指令，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。

7.6.2 非对称密码算法加密解密实现正确性测试

测试步骤如下：

a) 导出公钥，对数据进行卡外加密；
b) 执行非对称密码算法解密运算指令，还原明文数据进行解密验证；
c) 将测试公钥导入到卡内，执行非对称密码算法加密运算指令；
d) 将加密数据在卡外进行解密，还原明文数据进行加密验证；
e) 运算结果应能通过正确性验证。

7.6.3 非对称密码算法数字签名与签名验证实现正确性测试

测试步骤如下：

a) 执行数字签名算法运算指令；
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，执行签名验证算法运算指令；
e) 运算结果应能通过正确性验证。

7.6.4 杂凑密码算法实现正确性测试

测试步骤如下：

a) 使用随机数据，执行杂凑密码算法运算指令；

b） 返回运算结果，与预期结果进行比较；
c） 运算结果应能通过正确性验证。

7.6.5 非对称密码算法密钥生成正确性测试

测试步骤如下：
a） 生成公私钥对，应返回成功；
b） 使用公钥对特定数据加密，应返回成功；
c） 使用私钥对加密结果解密，应返回成功，运算结果应能通过正确性验证；

7.6.6 非对称密码算法密钥配对一致性测试

生成不少于 1 000 对密钥对，每次进行配对一致性检测。配对一致性检测方法与 GM/T 0039 中的检测方法一致。

7.6.7 序列密码算法实现正确性测试

测试步骤如下：
a） 执行用序列密码算法的运算指令，用指定密钥进行运算；
b） 运算结果应能通过正确性验证。

7.7 密码算法实现性能检测

7.7.1 分组密码算法加密性能测试

测试步骤如下：
a） 预先产生 M 组（$M \geqslant 1\ 000$）随机数据和随机密钥，依次通过分组密码算法指令执行加密运算；
b） 验证加密结果正确性；
c） 累积运算时间 T；
d） 计算加密速率 V，其中每组数据的数据量为 B 比特，因此 $V=(M\times B)/T$（kbit/s 或 bit/s）。

注：1 kbit/s=1 000 bit/s。

7.7.2 分组密码算法解密性能测试

测试步骤如下：
a） 预先产生 M 组（$M \geqslant 1\ 000$）的随机数据和随机密钥，依次通过分组密码算法指令执行解密运算；
b） 验证解密结果正确性；
c） 累积运算时间 T；
d） 计算解密速率 V，其中每组数据的数据量为 B 比特，因此 $V=(M\times B)/T$（kbit/s 或 bit/s）。

7.7.3 非对称密码算法密钥对生成性能测试

测试步骤如下：
a） 连续生成 M 对（$M \geqslant 1\ 000$）公私钥对；
b） 累计运算时间 T；
c） 计算密钥对生成速率 V，$V=M/T$（密钥对/秒）。

7.7.4 非对称密码算法加密性能测试

测试步骤如下：

a) 预先产生 M 组($M \geqslant 1\ 000$)的随机数据和随机密钥,依次通过公钥加密算法指令执行加密运算;
b) 验证加密结果正确性;
c) 累积运算时间 T;
d) 计算加密速率 V,其中每组数据的数据量为 B 比特,因此 $V=(M\times B)/T$(kbit/s 或 bit/s)。

7.7.5 非对称密码算法解密性能测试

测试步骤如下:

a) 预先产生 M 组($M \geqslant 1\ 000$)的随机数据和随机密钥,依次通过公钥解密算法指令执行解密运算;
b) 验证结果正确性;
c) 累积运算时间 T;
d) 计算解密速率 V,其中每组数据的数据量为 B 比特,因此 $V=(M\times B)/T$(kbit/s 或 bit/s)。

7.7.6 非对称密码算法数字签名性能测试

测试步骤如下:

a) 预先产生 M 组($M \geqslant 1\ 000$)的随机数据和随机密钥,依次通过数字签名算法指令执行签名运算;
b) 验证结果正确性;
c) 累积运算时间 T;
d) 计算签名速率 V,其中每组数据的数据量为 B 比特,因此 $V=(M\times B)/T$(kbit/s 或 bit/s)。

7.7.7 非对称密码算法签名验证性能测试

测试步骤如下:

a) 预先产生 M 组($M \geqslant 1\ 000$)的随机数据和随机密钥,依次通过签名验证算法指令执行签名验证运算;
b) 验证结果正确性;
c) 累积运算时间 T;
d) 计算签名验证速率 V,其中每组数据的数据量为 B 比特,因此 $V=(M\times B)/T$(kbit/s 或 bit/s)。

7.7.8 杂凑密码算法实现性能测试

测试步骤如下:

a) 变化数据长度,从 1 字节到 N 字节($N>128$),每数据长度预先产生不少于 8 条随机数据,总预先产生 M 条($M \geqslant 1\ 000$)随机数据,依次通过密码杂凑算法指令执行运算;
b) 验证计算结果;
c) 累积运算时间 T;
d) 计算杂凑速率 V,因此 $V=M/T$(bit/s)。

7.7.9 序列密码算法加密性能测试

测试步骤如下:

a) 预先产生 M 组($M \geqslant 1\ 000$)的随机数据和随机密钥,依次执行序列密码算法指令进行加密运算;
b) 验证加密结果正确性;

c) 累积运算时间 T；

d) 计算加密速率 V，其中每组数据的数据量为 B 比特，因此 $V=(M\times B)/T$（kbit/s 或 bit/s）。

7.7.10 序列密码算法解密性能测试

测试步骤如下：

a) 预先产生 M 组（$M\geqslant 1\ 000$）的随机数据和随机密钥，依次执行序列密码算法指令进行解密运算；

b) 验证解密结果正确性；

c) 累积运算时间 T；

d) 计算解密速率 V，其中每组数据的数据量为 B 比特，因此 $V=(M\times B)/T$（kbit/s 或 bit/s）。

7.7.11 序列密码算法完整性性能测试

测试步骤如下：

a) 预先产生 M 组（$M\geqslant 1\ 000$）的随机数据和随机密钥，依次执行序列密码算法指令进行完整性运算；

b) 验证完整性结果正确性；

c) 累积运算时间 T；

d) 计算完整性速率 V，其中每组数据的数据量为 B 比特，因此 $V=(M\times B)/T$（kbit/s 或 bit/s）。

7.8 设备安全性测试

智能 IC 卡安全性测试方法按照 GM/T 0039。

8 送检技术文档要求

按国家密码管理主管部门检测要求提交相关文档资料，作为检测依据。文档资料应包含但不限于以下内容。

a) 技术工作总结报告。

b) 安全性设计报告：应详细描述产品的安全设计，包括遵循的最小权限原则。最小权限原则是指智能 IC 卡在所有操作过程中应当限制在完成特定任务所需的最低权限范围内。

c) 用户手册。

此外，如果送检产品提供了为测试独立开放的测试接口指令，需在送检文档中明确说明该接口仅用于检测目的，不应用于其他任何用途，并在检测完毕后予以失效。

9 判定规则

测试对象应完全符合以下条件，方可判定为合格；如不符合任何一项，则按规定视为不合格。

a) 应使用符合国家密码管理要求的密码算法。

b) 应通过 7.2 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 7.2.1 规定的测试；

2) 如测试对象支持内部认证命令，应通过 7.2.2 规定的测试；

3) 如测试对象支持 PIN 认证命令，应通过 7.2.3 规定的测试；

4) 如测试对象支持 PIN 修改命令，应通过 7.2.3 和 7.2.4 规定的测试；

5) 如测试对象支持 PIN 重装命令，应通过 7.2.3 和 7.2.5 规定的测试；

6） 如测试对象支持 PIN 解锁命令，应通过 7.2.3 和 7.2.6 规定的测试。

c） 应通过 7.3 的所有相关测试，包括多应用支持（如有）。

d） 如支持 RSA 密钥对生成，应通过 7.4 测试。

e） 应通过 7.5 测试。

f） 应通过 7.6 中与支持算法相关的测试。

参 考 文 献

[1] GB/T 16649.3—2024 识别卡 集成电路卡 第3部分:带触点的卡电接口和传输协议
[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—2023 SM2密码算法使用规范
[5] GM/T 0010—2023 SM2密码算法加密签名消息语法规范
[6] GM/T 0028—2024 密码模块安全技术要求

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—2024
*
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)
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 1.5　字数 33 千字
2025年6月第1版　2025年6月第1次印刷
*
书号:155066·2-39097　定价 43.00 元

GM/T 0041-2024