

团 体 标 准

T/ZSA 67.4-2019

# 移动智能终端密码模块技术框架

## 第 4 部分：密钥多端协同计算保护技术架构

Technical framework of cryptographic module in mobile smart terminal

Part 4: Key protection based on multi-party computation

2019-12-31 发布

2020-03-01 实施

中关村标准化协会 发布

## 目 次

前言.....	II
引言.....	III
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 符号和缩略语.....	3
5 概述.....	3
5.1 引言.....	3
5.2 密钥双端协同计算保护.....	3
5.3 密钥三端协同计算保护.....	5
6 密码模块规格.....	7
6.1 密码模块类型.....	7
6.2 密码边界.....	7
6.3 工作模式.....	8
7 密码模块接口.....	8
8 角色、服务和鉴别.....	8
8.1 角色.....	8
8.2 服务.....	9
8.3 鉴别.....	9
9 软件/固件安全.....	9
10 运行环境.....	9
11 物理安全.....	9
12 非侵入式安全.....	9
13 敏感安全参数管理.....	10
13.1 概述.....	10
13.2 随机比特生成器.....	10
13.3 敏感安全参数的生成.....	10
13.4 敏感安全参数的建立.....	10
13.5 敏感安全参数的输入输出.....	10
13.6 敏感安全参数的存储.....	10
13.7 敏感安全参数置零.....	11
14 自测试.....	11
15 生命周期保障.....	11
16 对其他攻击的缓解.....	11
附录 A (资料性附录) 应用示例.....	12
附录 B (参考性附录) SM2 双端协同计算流程示例.....	14
附录 C (参考性附录) SM2 三端协同计算流程示例.....	17
参考文献.....	20

## 前 言

T/ZSA 67-2019《移动智能终端密码模块技术框架》分为5个部分：

第1部分：总则

第2部分：密钥加密本地保护技术架构

第3部分：密钥加密云保护技术架构

第4部分：密钥多端协同计算保护技术架构

第5部分：基于安全芯片的技术架构

本部分为 T/ZSA 67-2019《移动智能终端密码模块技术框架》的第4部分。

本部分按照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。中关村标准化协会不承担识别这些专利的责任。

本部分由中关村标准化协会技术委员会提出并归口。

本部分主要起草单位：中关村网络安全与信息化产业联盟、北京江南天安科技有限公司、中国科学院信息工程研究所、奇安信科技集团股份有限公司、江苏通付盾科技有限公司、北京握奇数据股份有限公司、卫士通信息产业股份有限公司、鼎桥通信技术有限公司等。

本部分主要起草人：刘宗斌、张晶、李强、王克、史晗晖、张凡、傅文斌、李勃、鲁洪成、李向荣、张令臣等。