ICS 35.240
L70/84

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

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。