



中华人民共和国国家标准

GB/T 38636—2020

信息安全技术 传输层密码协议(TLCP)

Information security technology—Transport layer cryptography protocol(TLCP)

2020-04-28 发布

2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	I
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	1
5 密码算法和密钥种类	2
5.1 概述	2
5.2 密码算法	3
5.3 密钥种类	3
6 协议	4
6.1 概述	4
6.2 数据类型定义	4
6.3 记录层协议	5
6.4 握手协议族	10
6.5 密钥计算	23
附录 A (规范性附录) GCM 可鉴别加密模式	24
参考文献	31

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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:山东得安信息技术有限公司、格尔软件股份有限公司、北京信安世纪科技有限公司、成都卫士通信息产业股份有限公司、长春吉大正元信息技术股份有限公司、北京握奇智能科技有限公司、北京三未信安科技发展有限公司、北京海泰方圆科技有限公司、国家密码管理局商用密码检测中心、北京江南天安科技有限公司、中金金融认证中心有限公司、北京天融信网络安全技术有限公司。

本标准主要起草人:郑强、马洪富、汪宗斌、罗俊、赵丽丽、张立廷、汪雪林、田敏求、张岳公、蒋红宇、吕春梅、李国、孙圣男、雷晓锋。