第1章 移动通信系统的安全基础

1.1 加密算法与WPKI …… 1
1.1.1 加密算法与RSA …… 1
1.1.2 PKI与WPKI …… 7
1.1.3 AES加密算法简介 …… 14
1.2 签名与认证 …… 19
1.2.1 椭圆曲线简介 …… 19
1.2.2 移动网络数字签名 …… 23
1.2.3 基于ECC的签密方案 …… 35
1.3 密钥管理与协商 …… 38
1.3.1 基于椭圆曲线密码的可认证密钥协商 …… 38
1.3.2 基于证书公钥的单方签名可认证密钥协商 …… 43
1.3.3 基于身份公钥的可认证密钥协商 …… 48
1.3.4 基于自证明公钥的可认证密钥协商 …… 57
1.4 伪随机数发生器 …… 63
1.4.1 伪随机序列发生器 …… 63
1.4.2 高速伪随机数发生器 …… 65
1.4.3 动态并行反馈移位寄存器的实现 …… 66
1.4.4 伪随机比特发生器 …… 68
本章参考文献 …… 72

第2章 第二代移动通信系统安全技术

2.1 GSM的安全体系 …… 74
2.1.1 GSM网络概述 …… 74
2.1.2 GSM网络的安全体系结构 …… 75
2.1.3 GSM网络的身份认证 …… 78
2.1.4 GSM网络存在的安全缺陷及相关攻击方法 …… 80

2.2 GPRS 的安全体系 …… 86
2.2.1 GPRS 网络简介 …… 87
2.2.2 GPRS 系统的安全体系结构 …… 87
2.2.3 GPRS 系统的安全服务和安全威胁 …… 88
2.3 COMP128 算法的安全性分析 …… 89
2.3.1 COMP128 算法介绍 …… 90
2.3.2 对 COMP128 算法的攻击 …… 91
2.3.3 对 COMP128 算法的安全改进 …… 97
2.4 IS-41 的安全体系 …… 103
2.4.1 2G 的信任模型和认证场合 …… 104
2.4.2 IS-41 接入安全机制 …… 105
2.4.3 对 IS-41 接入安全机制的攻击 …… 110
2.4.4 2G 安全的比较 …… 113
本章参考文献 …… 116

第 3 章 第三代移动通信系统安全技术

3.1 WCDMA 接入安全 …… 118
3.1.1 WCDMA 系统接入安全内容 …… 118
3.1.2 WCDMA 网络安全机制 …… 122
3.1.3 安全链接建立过程 …… 132
3.1.4 WCDMA 认证算法分析与改进 …… 136
3.2 CDMA2000 接入安全 …… 145
3.2.1 CDMA2000 系统接入安全内容 …… 145
3.2.2 CDMA2000 安全特征 …… 146
3.2.3 A-Key 协商机制 …… 152
3.2.4 CDMA2000 与 WCDMA 接入安全评估比较 …… 156
3.3 移动通信系统核心网的安全 …… 159
3.3.1 移动通信核心网的安全需求 …… 159
3.3.2 MAP 协议的安全保护 …… 159
3.3.3 IP 网络层安全 …… 163
3.3.4 认证架构 …… 166
本章参考文献 …… 168

第 4 章 WAP 安全

4.1 WAP 架构 …… 171

4.1.1 WAP 模型 …… 171
4.1.2 WAP 协议栈 …… 172
4.2 WTLS …… 173
4.2.1 TLS 协议 …… 173
4.2.2 WTLS 协议对 TLS 协议的修改 …… 177
4.2.3 WTLS 协议分析 …… 183
4.2.4 传输层安全 …… 187
4.3 WMLSCrypto …… 190
4.3.1 WMLScript …… 190
4.3.2 JavaScript 的 Crypto 对象 …… 191
4.3.3 WMLCrypto …… 191
4.3.4 WMLSCrypto 的应用和发展 …… 192
4.4 WIM …… 192
4.4.1 PKCS#15 …… 193
4.4.2 WIM …… 194
4.4.3 WIM 的应用 …… 195
4.4.4 MeT 框架 …… 197
本章参考文献 …… 198

第 5 章 TETRA 安全技术

5.1 TETRA 数字集群系统 …… 201
5.1.1 数字集群系统简介 …… 201
5.1.2 TETRA 系统标准、技术特性及业务类型 …… 202
5.1.3 TETRA 网络结构 …… 204
5.1.4 TETRA 系统的安全性 …… 205
5.2 TETRA 系统鉴权及空中接口加密 …… 207
5.2.1 TETRA 系统的基本鉴权过程 …… 207
5.2.2 TETRA 鉴权的安全性分析 …… 212
5.2.3 鉴权密钥分配(AKD) …… 213
5.2.4 TETRA 系统空中接口加密 …… 218
5.3 TETRA 系统端到端保密通信 …… 220
5.3.1 加密算法 …… 221
5.3.2 同步帧 …… 223
5.3.3 端到端保密通信 …… 225

5.3.4 TETRA 安全群组通信的密钥管理 …… 227
5.4 TETRA 系统的密钥管理中心 …… 242
5.4.1 KMC 功能描述 …… 242
5.4.2 KMC 处理流程分析 …… 242
5.4.3 KMC 的实现 …… 254
本章参考文献 …… 259

第 6 章 WLAN 安全技术

6.1 WLAN 安全机制 …… 262
6.1.1 802.11 标准的安全机制 …… 262
6.1.2 WLAN 安全机制的改进 …… 265
6.1.3 WLAN 安全机制的缺陷 …… 269
6.1.4 WLAN 的安全策略 …… 274
6.2 基于 IPSec 的 WLAN 安全系统设计 …… 279
6.2.1 IPSec 体系结构 …… 279
6.2.2 系统需求分析 …… 282
6.2.3 系统体系结构 …… 283
6.2.4 核心功能模块实现 …… 285
6.3 基于 3GPP AKA 的 WLAN 接入认证 …… 290
6.3.1 WLAN 与 3G 的互补性 …… 290
6.3.2 WLAN 与 3G 的互通模型 …… 291
6.3.3 基于 3GPP AKA 的 WLAN 安全接入 …… 293
6.4 基于安全嵌入式平台的 WLAN 安全解决方案 …… 296
6.4.1 安全方案 …… 296
6.4.2 WLAN 安全嵌入系统的设计 …… 298
6.4.3 安全嵌入式平台所能解决的安全问题 …… 299
本章参考文献 …… 300

第 7 章 无线通信安全新挑战

7.1 电话网攻击 …… 303
7.1.1 电话网安全问题 …… 303
7.1.2 拒绝服务攻击 …… 308
7.1.3 账户口令窃取 …… 310
7.1.4 针对信令网的攻击 …… 311
7.2 手机病毒 …… 312

7.2.1 手机操作系统概论 …… 312
7.2.2 短信类手机病毒 …… 314
7.2.3 炸弹类手机病毒 …… 315
7.2.4 蠕虫类手机病毒 …… 315
7.2.5 木马类手机病毒 …… 316
7.3 SIM 卡攻击 …… 317
7.3.1 针对手机漏洞的短消息攻击 …… 317
7.3.2 针对 SIM 卡短消息协议处理漏洞的攻击 …… 318
7.3.3 利用短消息网站漏洞的拒绝服务攻击 …… 318
7.3.4 直接拒绝服务攻击 …… 320
7.3.5 SIM 卡旁路攻击 …… 320
7.3.6 伪装手机实施 SIM 卡攻击 …… 321
7.3.7 伪装基站实施 SIM 卡攻击 …… 324
7.4 移动多媒体版权保护 …… 325
7.4.1 数字水印版权管理系统原理 …… 325
7.4.2 WDRM 安全性分析 …… 328
本章参考文献 …… 329
后记 …… 334