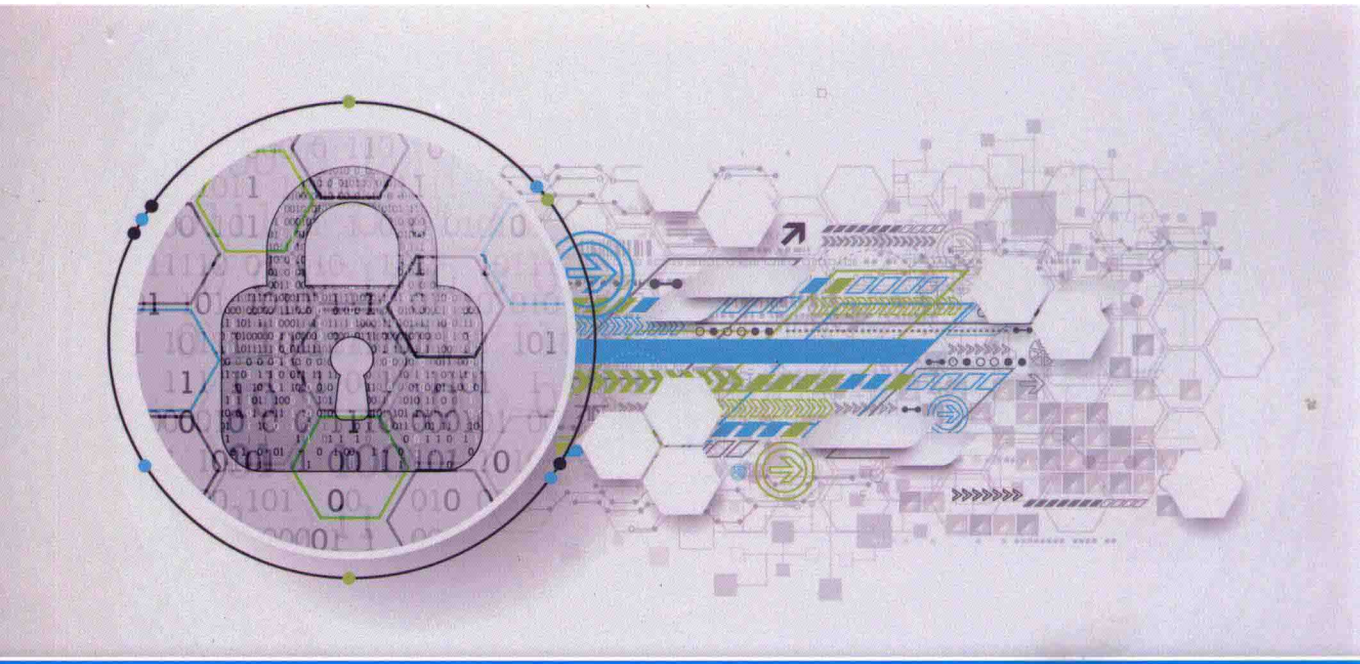
高等院校网络空间安全系列规划教材



安全协议（第2版）

曹天杰　张凤荣　汪楚娇◎编著

ANQUAN XIEYI

北京邮电大学出版社
www.buptpress.com

高等院校网络空间安全系列规划教材

安 全 协 议

(第2版)

曹天杰 张凤荣 汪楚娇 编著

北京邮电大学出版社
www.buptpress.com

内 容 简 介

本书全面、系统地讲述了安全协议的基本理论、安全协议的主要类型以及安全协议的设计与分析方法。围绕机密性、完整性、认证性、非否认性、匿名性、公平性等实际需求，较全面地介绍了满足各种应用需要的安全协议。本书反映了安全协议领域的新成果，介绍了移动互联网中广泛使用的图形口令和扫码登录、比特币中的区块链技术、云计算中的云存储协议和外包计算协议、物联网中的 RFID 协议、量子计算中的量子密钥分发协议等。

本书主要内容包括：安全协议概述、安全协议的密码学基础、基本的安全协议、认证与密钥建立协议、零知识证明、选择性泄露协议、数字签名变种、非否认协议、公平交换协议、安全协议的应用、安全多方计算、安全协议的形式化分析。

本书内容全面、选材适当、实例丰富、概念准确、逻辑性强。本书不仅可以作为网络空间安全专业本科生和研究生的教材，也可以作为网络空间安全领域科研人员的参考书。

图书在版编目(CIP)数据

安全协议 / 曹天杰，张凤荣，汪楚娇编著. -- 2 版. -- 北京 ：北京邮电大学出版社，2020.9

ISBN 978-7-5635-6203-9

Ⅰ. ①安… Ⅱ. ①曹… ②张… ③汪… Ⅲ. ①计算机网络—安全技术—通信协议 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2020)第 171754 号

策划编辑：马晓仟　　**责任编辑**：刘春棠　　**封面设计**：七星博纳

出版发行：北京邮电大学出版社

社　　址：北京市海淀区西土城路 10 号

邮政编码：100876

发 行 部：电话：010-62282185　传真：010-62283578

E-mail：publish@bupt.edu.cn

经　　销：各地新华书店

印　　刷：保定市中画美凯印刷有限公司

开　　本：787 mm×1 092 mm　1/16

印　　张：14.5

字　　数：378 千字

版　　次：2009 年 8 月第 1 版　2020 年 9 月第 2 版

印　　次：2020 年 9 月第 1 次印刷

ISBN 978-7-5635-6203-9　　定价：38.00 元

前言

Foreword

密码学的用途是解决现实世界中的种种难题。当我们考虑具体应用时，常常遇到以下安全需求：机密性、完整性、认证性、非否认性、匿名性、公平性等，密码学解决的各种难题围绕这些安全需求。安全协议是使用密码学完成某项特定的任务并满足安全需求的协议，又称密码协议，它在网络和分布式系统中有着大量的应用。

安全协议使用伪随机生成器、分组密码算法、消息认证码、哈希算法、公钥加密与签名算法等密码原语构造，这些密码原语好比是砖块，安全协议就是利用砖块建筑的具有不同功能的大楼，比如写字楼、游泳馆、住宅等。我们知道即使砖块是结实的，如果设计不好，大楼也是容易倒塌的。本书讲解如何利用密码原语这些砖块构建一座座既要提供各种不同功能，又要安全牢固的大楼。

“安全协议”课程是“密码学”的后续课程，网络空间安全专业大多设置了该课程。《安全协议》第1版于2009年出版，近年来，移动互联网、区块链、云计算、物联网、量子计算等得到了飞速发展，安全协议也在这些领域得到了深入应用，因此，对《安全协议》进行改版很有必要。

本版教材的修改原则是保持第1版的基本面貌与知识结构，在此基础上修改、补充，使内容更为全面、选材更加新颖、基本理论与实例结合更为紧密。

本版教材补充的主要内容包括：时间戳协议、密钥托管、扫码登录、开放授权OAuth、图形口令概述、基于识别的图形口令、基于回忆的图形口令、混合型图形口令、验证码概述、验证码分类、Pinkas-Sander协议、聚合签名、比特币概述、比特币原理、比特币的安全性、云存储数据的持有性证明、云存储数据的可搜索加密、基于属性加密的云数据共享、基于代理重加密的云数据共享、云计算环境下的外包计算、量子密码基础、BB84协议，反映了安全协议领域的最新进展。此外，每章适当增加了新的例题与习题。

本版教材保持第1版的特色不变，内容有所增加。本版教材特色如下。

(1) 内容全面。本版教材系统地讲述了安全协议的基本理论，在明确安全需求的基础上，由浅入深地介绍了各类安全协议，包括经典协议(即使有缺陷)、标准化的协议、广泛应用的协议。针对应用中可能面临的各类攻击，介绍了经典的安全协议设计与分析方法，最后一章介绍了安全协议的形式化分析方法。

（2）选材适当、实例丰富。作者长期从事安全协议方面的研究，把安全协议领域的新成果引入本版教材，如移动互联网中广泛使用的图形口令和扫码登录、比特币中的区块链技术、云计算中的云存储协议和外包计算协议、量子计算中的量子密钥分发协议等。当一类安全协议提出后，根据不同的应用环境、面临的不同安全威胁，人们会提出各种相对应的协议。作为教材，不可能面面俱到地把每种协议都介绍给读者，因此，根据难度、应用的广泛性选取有代表性的协议非常重要。本版教材选材主要是经典场景下的典型协议，读者通过对典型协议的学习，能够融会贯通，在将来的学术研究及实际应用中设计出面向新问题的协议。书中实例主要来自学术论文，实例具有典型性，难度适当。

（3）概念准确、逻辑性强。本版教材从应用场景对应的安全需求、安全威胁及协议设计目标出发，提出相应的协议概念，进而设计协议并给出安全性分析。在介绍早期协议存在的缺陷基础上，再介绍改进后的协议，能够让学生理解设计协议的整个思路。在章节安排上，注意由浅入深、前后连贯。例如，时间戳协议中的链接协议是区块链的雏形，承诺方案在认证协议和签名协议中用到，具有特殊性质的签名协议在电子现金和电子拍卖协议中得到应用。

本版教材共分为12章，第1章是安全协议概述，第2章介绍安全协议的密码学基础。从第3章开始，阐述安全协议中的一些基本理论和关键技术：基本的安全协议、认证与密钥建立协议、零知识证明、选择性泄露协议、数字签名变种、非否认协议、公平交换协议、安全协议的应用、安全多方计算、安全协议的形式化分析。我们希望，通过学习本教材，读者可以对安全协议有一个全面深入的了解。

《安全协议》第1版被列入江苏省高等学校精品教材建设立项项目，本版教材所涉及的研究内容也得到国家自然科学基金（项目编号61972400）的资助。

本版教材可以作为网络空间安全专业本科生及研究生的教材，也可以供网络空间安全领域的科研人员参考。

由于作者水平有限，书中疏漏与错误之处在所难免，恳请广大同行和读者批评指正。作者联系方式为：tjcao@cumt.edu.cn，欢迎随时联系索取课程资料。

作　者

于中国矿业大学计算机科学与技术学院

2020年8月

目录

Contents

第 1 章　安全协议概述 …… 1

1.1　安全协议的概念 …… 1
1.1.1　协议、算法与安全协议 …… 1
1.1.2　协议运行环境中的角色 …… 2
1.2　常用的安全协议 …… 2
1.3　安全协议的安全性质 …… 3
1.4　对安全协议的攻击 …… 5
1.5　安全协议的三大理论分析方法 …… 8
1.5.1　安全多方计算 …… 8
1.5.2　形式化分析方法 …… 9
1.5.3　可证明安全性理论 …… 10
习题 1 …… 11

第 2 章　安全协议的密码学基础 …… 12

2.1　密码学的基本概念 …… 12
2.2　数论中的一些难题 …… 13
2.3　随机数 …… 13
2.4　分组密码 …… 14
2.5　公开密钥密码 …… 14
2.5.1　公开密钥密码的基本概念 …… 15
2.5.2　RSA 体制 …… 15
2.5.3　Rabin 体制 …… 16
2.6　哈希函数 …… 17
2.7　消息认证 …… 17
2.8　数字签名 …… 18
2.8.1　数字签名的基本概念 …… 18
2.8.2　RSA 签名 …… 19
2.8.3　数字签名标准 …… 20

2.8.4 ElGamal 数字签名 …… 21
2.8.5 Schnorr 签名体制 …… 21
2.8.6 基于椭圆曲线的数字签名算法 …… 22
2.9 基于身份的公钥密码学 …… 23
2.9.1 基于身份的加密方案 …… 23
2.9.2 基于身份的签名方案 …… 24
习题 2 …… 24

第 3 章 基本的安全协议 …… 26

3.1 秘密分割 …… 26
3.2 秘密共享 …… 26
3.3 阈下信道 …… 28
3.3.1 阈下信道的概念 …… 28
3.3.2 基于 ElGamal 数字签名的阈下信道方案 …… 30
3.3.3 基于 RSA 数字签名的阈下信道方案 …… 30
3.4 时间戳协议 …… 31
3.5 比特承诺 …… 32
3.5.1 使用对称密码算法的比特承诺 …… 32
3.5.2 使用单向函数的比特承诺 …… 33
3.5.3 使用伪随机序列发生器的比特承诺 …… 33
3.6 公平的硬币抛掷 …… 33
3.6.1 单向函数抛币协议 …… 34
3.6.2 公开密钥密码抛币协议 …… 34
3.7 智力扑克 …… 35
3.7.1 基本的智力扑克游戏 …… 35
3.7.2 三方智力扑克 …… 36
3.8 密钥托管 …… 36
3.9 不经意传输 …… 37
习题 3 …… 39

第 4 章 认证与密钥建立协议 …… 41

4.1 认证与密钥建立协议简介 …… 41
4.1.1 协议结构 …… 41
4.1.2 协议目标 …… 42
4.1.3 新鲜性 …… 43
4.2 使用共享密钥密码的协议 …… 43
4.2.1 实体认证协议 …… 44
4.2.2 无服务器密钥建立 …… 45

4.2.3　基于服务器的密钥建立 …… 46
4.2.4　使用多服务器的密钥建立 …… 50
4.3　使用公钥密码的认证与密钥传输 …… 51
4.3.1　实体认证协议 …… 51
4.3.2　密钥传输协议 …… 53
4.4　密钥协商协议 …… 58
4.4.1　Diffie-Hellman 密钥协商 …… 58
4.4.2　有基本消息格式的基于 DH 交换的协议 …… 61
4.4.3　增强消息格式的 DH 交换协议 …… 62
4.5　可证明安全的认证协议 …… 64
4.6　基于口令的协议 …… 65
4.6.1　口令协议概述 …… 65
4.6.2　使用 Diffie-Hellman 进行加密密钥交换 …… 66
4.6.3　强化的 EKE …… 67
4.6.4　双因子认证 …… 68
4.6.5　扫码登录 …… 69
4.6.6　开放授权 OAuth …… 70
4.7　基于图形口令的认证 …… 71
4.7.1　图形口令概述 …… 72
4.7.2　基于识别的图形口令 …… 72
4.7.3　基于回忆的图形口令 …… 73
4.7.4　混合型图形口令 …… 75
4.8　基于验证码的认证 …… 76
4.8.1　验证码概述 …… 76
4.8.2　验证码的分类 …… 78
4.8.3　Pinkas-Sander 协议 …… 82
4.9　具有隐私保护的认证密钥交换协议 …… 82
4.9.1　可否认的认证密钥交换协议 …… 83
4.9.2　通信匿名的认证密钥交换协议 …… 83
4.9.3　用户匿名的认证密钥交换协议 …… 84
4.10　会议密钥协商 …… 84
习题 4 …… 87

第 5 章　零知识证明 …… 90

5.1　零知识证明的概念 …… 90
5.1.1　零知识证明的简单模型 …… 90
5.1.2　交互式零知识证明 …… 91
5.1.3　非交互零知识证明 …… 92

5.2 零知识证明的例子 …… 93
5.2.1 平方根问题的零知识 …… 93
5.2.2 离散对数问题的零知识证明 …… 93
5.3 知识签名 …… 94
5.4 身份鉴别方案 …… 95
5.4.1 身份的零知识证明 …… 96
5.4.2 简化的 Feige-Fiat-Shamir 身份鉴别方案 …… 97
5.4.3 Feige-Fiat-Shamir 身份鉴别方案 …… 97
5.4.4 Guillo-Quisquater 身份鉴别方案 …… 98
5.4.5 Schnorr 身份鉴别方案 …… 98
5.5 NP 语言的零知识证明 …… 99
习题 5 …… 100

第 6 章 选择性泄露协议 …… 101

6.1 选择性泄露的概念 …… 101
6.1.1 单一数字证书内容泄露 …… 101
6.1.2 多个数字证书内容泄露 …… 102
6.2 使用 Hash 函数的选择性泄露协议 …… 103
6.3 改进的选择性泄露协议 …… 105
6.3.1 Merkle 树方案 …… 105
6.3.2 Huffman 树方案 …… 106
6.4 数字证书出示中的选择性泄露 …… 108
6.4.1 签名证明 …… 108
6.4.2 选择性泄露签名证明 …… 110
习题 6 …… 112

第 7 章 数字签名变种 …… 113

7.1 不可否认签名 …… 113
7.2 盲签名 …… 115
7.2.1 RSA 盲签名方案 …… 115
7.2.2 Schnorr 盲签名方案 …… 116
7.3 部分盲签名 …… 116
7.4 公平盲签名 …… 117
7.5 一次性数字签名 …… 118
7.6 群签名 …… 119
7.7 环签名 …… 120
7.8 代理签名 …… 122
7.9 批验证与批签名 …… 123

7.9.1 批验证 …… 123
7.9.2 批签名 …… 124
7.10 聚合签名 …… 127
7.11 认证加密 …… 127
7.12 签密 …… 128
7.13 其他数字签名 …… 129
7.13.1 失败-终止签名 …… 129
7.13.2 指定验证者签名 …… 130
7.13.3 记名签名 …… 130
7.13.4 具有消息恢复功能的数字签名 …… 131
7.13.5 多重签名 …… 131
7.13.6 前向安全签名 …… 132
7.13.7 门限签名 …… 133
7.13.8 基于多个难题的数字签名方案 …… 133
习题 7 …… 133

第 8 章 非否认协议 …… 136

8.1 非否认协议的基本概念 …… 136
8.1.1 非否认服务 …… 136
8.1.2 非否认协议的步骤和性质 …… 137
8.1.3 一个非否认协议的例子 …… 138
8.2 无 TTP 参与的非否认协议 …… 139
8.2.1 Markowitch 和 Roggeman 协议 …… 140
8.2.2 Mitsianis 协议 …… 140
8.3 基于 TTP 参与的非否认协议 …… 141
8.3.1 TTP 的角色 …… 141
8.3.2 Zhou-Gollman 协议 …… 141
8.3.3 Online TTP 非否认协议——CMP1 协议 …… 142
习题 8 …… 143

第 9 章 公平交换协议 …… 145

9.1 公平交换协议的基本概念 …… 145
9.1.1 公平交换协议的定义 …… 145
9.1.2 公平交换协议的基本模型 …… 145
9.1.3 公平交换协议的基本要求 …… 146
9.2 同时签约 …… 146
9.2.1 带有仲裁者的同时签约 …… 147
9.2.2 无仲裁者的同时签约(面对面) …… 147

9.2.3 无仲裁者的同时签约(非面对面) …… 148
9.2.4 无须仲裁者的同时签约(使用密码技术) …… 148
9.3 数字证明邮件 …… 150
9.4 秘密的同时交换 …… 151
习题 9 …… 152

第 10 章 安全协议的应用 …… 153

10.1 电子选举 …… 153
10.1.1 简单投票协议 …… 153
10.1.2 使用盲签名的投票协议 …… 154
10.1.3 带两个中央机构的投票协议 …… 155
10.1.4 FOO 协议 …… 155
10.1.5 无须投票中心的投票协议 …… 158
10.2 电子现金 …… 160
10.2.1 电子现金的概念 …… 160
10.2.2 电子现金的优缺点 …… 161
10.2.3 电子现金的攻击和安全需求 …… 161
10.2.4 使用秘密分割的电子现金协议 …… 163
10.2.5 基于 RSA 的电子现金协议 …… 164
10.2.6 Brands 电子现金协议 …… 165
10.3 比特币 …… 166
10.3.1 比特币概述 …… 166
10.3.2 比特币的原理 …… 167
10.3.3 比特币的安全性 …… 172
10.4 电子拍卖 …… 173
10.4.1 电子拍卖系统的模型和分类 …… 173
10.4.2 电子拍卖的过程 …… 173
10.4.3 电子拍卖的安全需求 …… 174
10.4.4 NFW 电子拍卖协议 …… 174
10.4.5 NPS 电子拍卖协议 …… 175
10.5 云计算 …… 176
10.5.1 云存储数据的持有性证明 …… 176
10.5.2 云存储数据的可搜索加密 …… 181
10.5.3 基于属性加密的云数据共享 …… 183
10.5.4 基于代理重加密的云数据共享 …… 185
10.5.5 云计算环境下的外包计算 …… 186
10.6 物联网 …… 187
10.6.1 RFID 系统的基本构成 …… 188

10.6.2　RFID 系统的安全需求 …… 189
10.6.3　RFID 认证协议 …… 190
10.7　量子密钥分发 …… 195
10.7.1　量子密码基础 …… 195
10.7.2　BB84 协议 …… 196
习题 10 …… 198

第 11 章　安全多方计算 …… 200

11.1　安全多方计算的概念 …… 200
11.2　安全多方计算的需求 …… 202
11.2.1　安全多方计算的安全需求 …… 202
11.2.2　用于函数的安全多方计算协议的要求 …… 203
11.3　多方计算问题举例 …… 203
11.3.1　点积协议 …… 203
11.3.2　“百万富翁”协议 …… 204
11.3.3　密码学家晚餐问题 …… 205
11.4　一般安全多方计算协议 …… 206
习题 11 …… 207

第 12 章　安全协议的形式化分析 …… 209

12.1　形式化方法简介 …… 209
12.2　安全协议形式化分析的历史 …… 210
12.3　安全协议形式化分析的分类 …… 211
12.3.1　定理证明方法 …… 212
12.3.2　模拟检测方法 …… 212
12.3.3　互模拟等价 …… 213
12.4　基于逻辑推理的方法和模型 …… 213
12.4.1　BAN 逻辑的构成 …… 213
12.4.2　理想化协议 …… 215
12.4.3　示例分析 …… 216
习题 12 …… 218

参考文献 …… 219

第 1 章 安全协议概述

安全协议是为了解决网络中的现实问题而设计的协议。本章阐述了安全协议的概念，分析了安全协议设计与分析所面临的问题，介绍了安全协议的理论分析方法。

1.1 安全协议的概念

安全协议(Security Protocol)又称密码协议(Cryptographic Protocol)，是以密码学为基础的消息交换协议，其目的是在网络环境中提供各种安全服务。

1.1.1 协议、算法与安全协议

在理解安全协议这一概念之前，首先要了解什么是协议。所谓协议，就是两个或两个以上的参与者采取一系列步骤以完成某项特定的任务，如 Internet 中的 IP 协议、TCP 协议、FTP 协议，现实生活中的购房协议、棋牌游戏规则等。这个定义有以下三层含义：

(1) 协议需要两个或两个以上的参与者。一个人可以通过执行一系列的步骤来完成一项任务，但不构成协议。

(2) 在参与者之间呈现为消息处理和消息交换交替进行的一系列步骤。

(3) 通过执行协议必须能够完成某项任务或达成某项共识。

另外，协议还有以下特点：

(1) 协议中的每个参与者都必须了解协议，并且预先知道所要完成的所有步骤。

(2) 协议中的每个参与者都必须同意并遵循它。

(3) 协议必须是清楚的，每一步必须明确定义，并且不会引起误解。

(4) 协议必须是完整的，对每种情况必须规定具体的动作。

协议与算法不同。算法应用于协议中消息处理的环节，不同的消息处理方式则要求不同的算法。

密码学的用途是解决各种难题。当我们考虑现实世界中的应用时，常常遇到以下安全需求：机密性、完整性、认证性、非否认性、匿名性、公平性等，密码学解决的各种难题都围绕这些安全需求。安全协议是使用密码学完成某项特定的任务并满足安全需求的协议，又称密码协议。在安全协议中，经常使用对称密码、公开密钥密码、单向函数、伪随机数生成器等密码算法，可以说，安全协议就是在消息处理环节采用了若干密码算法的协议。具体而言，密码算法为传递的消息提供高强度的加解密操作和其他辅助操作(如 Hash 运算)，而安全协议是在这些密码算法的基础上提供满足各种安全性要求的方案。安全协议中使用密码算法的目的是防

止、发现窃听和欺骗。

安全协议的目的是在网络环境中为用户提供各种安全服务。安全协议运行在计算机网络或分布式系统中，为各方提供一系列步骤，借助于密码算法来实现密钥分配、身份认证以及安全地完成电子交易。

依据安全协议产生的应用需求以及运行的环境，安全协议设计应遵循以下原则：

（1）安全协议应满足应用需求，如选举协议应能够完成选举，拍卖协议应能够完成拍卖。

（2）安全协议应满足安全需求，如选举协议中，不能泄露选票内容，选票不能被攻击者修改等。

（3）密码协议的运行应尽量简单高效，如较小的计算量、存储量、通信带宽，较少的交互次数。在保证达成应用需求目标和安全需求目标的情况下，协议应务求简单高效、可读性好。

1.1.2 协议运行环境中的角色

1. 参与者

协议执行过程中的双方或多方也就是我们常说的发送方和接收方。协议的参与者可能是完全信任的人，也可能是攻击者和完全不信任的人，如认证协议中的发起者和响应者，零知识证明中的证明人和验证者，电子商务中的商家、银行和客户等。通常使用 Alice 作为协议中的第一个参与者，Bob 作为协议中的第二个参与者，Carol 作为三、四方协议中的参与者。

2. 攻击者

攻击者（敌手）就是协议过程中企图破坏协议安全性和正确性的人。我们把不影响协议执行的攻击者称为被动攻击者，他们仅仅观察协议并试图获取信息。还有一类攻击者叫作主动攻击者，他们改变协议，在协议中引入新消息、修改消息或者删除消息等，达到欺骗、获取敏感信息、破坏协议等目的。通常使用 Eve 作为窃听者，Mallory 作为恶意的主动攻击者。

攻击者可能是协议的合法参与者、外部实体或两者的组合体，可能是单个实体，也可能是合谋的多个实体。协议参与者在协议期间撒谎，或者根本不遵守协议，这类攻击者叫作骗子，由于是系统的合法用户，因此也称为内部攻击者。攻击者也可能是外部的实体，他可能仅仅窃听以获取可用信息，也可能引入假冒的消息，这类攻击者称为外部攻击者。

3. 可信第三方

可信第三方（Trusted Third Party，TTP）是指在完成协议的过程中值得信任的第三方，能帮助互不信任的双方完成协议。仲裁者是一类特殊的可信第三方，用于解决协议执行中出现的纠纷。有时使用 Trent 表示仲裁者。仲裁者是在完成协议的过程中值得信任的公正的第三方，“公正”意味着仲裁者在协议中没有既得利益，对参与协议的任何人也没有特别的利害关系。“值得信任”表示协议中的所有人都接受仲裁的结果，即仲裁者说的都是真实的，他做的仲裁是正确的，并且他将完成协议中涉及他的部分。其他可信第三方如密钥分发中心、认证中心等。

1.2 常用的安全协议

最常用、最基本的安全协议主要有以下四类。

1. 密钥建立协议

在网络通信中，通常使用对称密码算法用单独的密钥对每一次单独的会话加密，这个密钥称为会话密钥。密钥建立协议的目的是在两个或者多个实体之间建立共享的会话密钥。可以采用对称密码体制或非对称密码体制建立会话密钥。可以借助于一个可信的服务器为用户分发密钥，这样的密钥建立协议称为密钥分发协议；也可以通过两个用户协商，共同建立会话密钥，这样的密钥建立协议称为密钥协商协议。

2. 认证协议

认证是对数据、实体标识的保证。数据起源认证意味着能够提供数据完整性，因为非授权地改变数据意味着数据来源的改变。实体认证是确认某个实体是它所声称的实体的过程，可能涉及证实用户的身份。认证协议主要防止假冒攻击。将认证和密钥建立协议结合在一起，是网络通信中最普遍应用的安全协议。

3. 电子商务协议

电子商务就是利用电子信息技术进行各种商务活动。电子商务协议中的主体往往代表交易的双方，其利益目标不一致。因此，电子商务协议最关注公平性，即协议应保证交易双方都不能通过损害对方利益而得到不应该得到的利益。常见的电子商务协议有电子现金协议、电子选举协议、拍卖协议等。

4. 安全多方计算协议

安全多方计算协议的目的是保证分布式环境中各参与方以安全的方式来共同执行分布式的计算任务。考虑到分布式计算的环境，在安全多方计算协议中，总假定协议在执行过程中会受到一个外部的实体，甚至是来自内部的一组参与方的攻击。这种假设很好地反映了网络环境下的安全需求。安全多方计算协议的两个最基本的安全要求是保证协议的正确性和各参与方私有输入的秘密性，即协议执行完后每个参与方都应该得到正确的输出，并且除此之外不能获知其他任何信息。安全多方计算协议包括：抛币协议、广播协议、选举协议、电子投标和拍卖协议、电子现金协议、合同签署协议、匿名交易协议、保密信息检索协议、保密数据库访问协议、联合签名协议、联合解密协议等。

根据是否有可信第三方的存在，协议又分为仲裁协议和自执行协议。

有可信第三方参与的协议，称为仲裁协议，但并不是在任何场景下都能找到可信的第三方。由于雇用仲裁者代价高昂，仲裁协议有时候可以分成两个低级的子协议，一个是非仲裁子协议，这个子协议是想要完成协议的各方每次都必须执行的；另一个是仲裁子协议，仅在例外的情况下执行，即有争议的时候才执行，这种特殊的仲裁者叫作裁决人，这样的协议称为裁决协议。

无可信第三方参与的协议称为自执行协议。由协议自身保证协议的公平性。协议的一方能够检测到另一方是否进行了欺骗，当检测到欺骗时，参与者可以终止协议的执行。由于协议设计的困难性，并不是任何情况下都能够设计出安全的自执行协议。

1.3　安全协议的安全性质

安全协议的目标就是保证某些安全性质在协议执行完毕时能够得以实现，换言之，评估一个安全协议是否是安全的就是检查其所要达到的安全性质是否受到攻击者的破坏。安全性质

主要有机密性、完整性、认证性、非否认性和公平性等。系统利用密码算法提供的安全性质也称为安全服务。

1. 机密性

机密性是指确保信息不暴露给未授权的实体或进程，即信息不会被未授权的第三方所知。非授权读是对机密性的破坏。

机密性的目的是保护协议消息不被泄露给非授权拥有此消息的人，即使是攻击者观察到了消息的格式，也无法从中得到消息的内容或提炼出有用的消息。保证协议消息机密性最直接的方法是对消息进行加密。加密使得消息由明文变为密文，并且任何人在不拥有密钥的情况下是不能解密消息的。

2. 完整性

完整性是指信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。非授权写是对完整性的破坏。

完整性的目的是保护协议消息不被非法改变、删除和替代。最常用的方法是封装和签名，即用签名或者 Hash 产生一个消息的摘要附在传送的消息上，作为验证消息完整性的依据，称为完整性校验值。一个关键性的问题是，通信双方必须事先达成有关算法的选择等款项的共识。

3. 认证性

认证可以对抗假冒攻击，用来确保身份，以便核查责任。在协议中，当某一成员（声称者）提交一个主体身份并声称它是那个主体时，需要运用认证以确认其身份是否如其声称所言，或者声称者需要拿出证明其真实身份的证据，这个过程称为认证的过程。在协议的实体认证中可以是单向的（认证一方），也可以是双向的（双方相互认证）。

4. 非否认性

非否认性是指收、发双方均不可否认（抵赖）已经发生的事实。一是源发证明，它提供给信息接收者以证据，这将使发送者谎称未发送过这些信息或者否认它的内容的企图不能得逞；二是交付证明，它提供给信息发送者以证据，这将使接收者谎称未接收过这些信息或者否认它的内容的企图不能得逞。

非否认性的目的是通过主体提供对方参与协议交换的证据以保证其合法利益不受侵害，即协议主体必须对自己的合法行为负责，而不能也无法事后否认。非否认协议的主体收集证据，以便事后能够向仲裁证明对方主体的确发送了或接收了消息。证据一般是以消息签名的形式出现的。

5. 公平性

公平性是电子支付协议的一个重要性质。其目的是保证参与协议的各方在协议执行的任何阶段都处于同等地位，当协议执行后，或者各方得到各自所需的，或者什么也得不到。

安全协议其他的安全性质还包括匿名与隐私属性、可验证性。在设计安全协议时，有时还要考虑各参与方的计算量、通信带宽、交互次数、存储量、强健性（鲁棒性）等。不同的系统有着不同的安全需求，如加密货币系统强调用户的匿名性，办公系统强调公文的机密性和完整性。对于有着不同角色使用的系统，各个角色的安全需求也是不同的，甚至是矛盾的，例如网络论坛，发帖人希望论坛提供匿名性，公安机关则要求论坛提供可追踪性。因此在设计具体系统的时候，要充分了解用户的安全需求，最终设计出既满足应用需求又满足安全需求的系统。

1.4　对安全协议的攻击

1983 年，Dolev 和 Yao(姚期智)发表了安全协议发展史上的一篇重要论文。该论文的主要贡献有两点。其一是将安全协议本身与安全协议采用的密码系统分开，在假定密码系统是“完善”的基础上讨论安全协议本身的正确性、安全性、冗余性等。从此，学者们可以专心研究安全协议的内在安全性质了。即问题很清楚地被划分为两个不同的层次：首先研究安全协议本身的安全性质，然后讨论实现层次的具体细节，包括所采用的具体密码算法等。

其二是 Dolev 和 Yao 建立了攻击者模型。他们认为，攻击者的知识和能力不能够低估，攻击者可以控制整个通信网络。Dolev 和 Yao 认为攻击者具有如下能力：

(1) 可以窃听所有经过网络的消息。

(2) 可以阻止和截获所有经过网络的消息。

(3) 可以存储所获得或自身创造的消息。

(4) 可以根据存储的消息伪造消息，并发送该消息。

(5) 可以作为合法的主体参与协议的运行。在此模型下，攻击者对网络有完全的控制权，可以在协议执行中的任何环节采取任何形式的攻击。

Dolev 和 Yao 的工作具有深远的影响。迄今为止，大部分有关安全协议的研究工作都遵循 Dolev 和 Yao 的基本思想。

对协议的攻击方法是多种多样的。对不同类型的安全协议，存在着不同的攻击，从而使协议达不到预定的安全目标，并且新的攻击方法也在不断产生。另外，对安全协议施加各种可能的攻击来测试其安全性也是常用手段之一。表 1.1 列出一些典型攻击并作了定义。

表 1.1　协议攻击类型

窃听	攻击者获取协议运行中所传输的消息
篡改	攻击者更改协议运行中所传输的消息的内容
重放	攻击者记录已经获取的消息并在随后的协议运行中发送给相同的或不同的接收者
预重放	攻击者在合法用户运行协议之前参与一次协议的运行
反射	攻击者将消息发回给消息的发送者
拒绝服务	攻击者阻止合法用户完成协议
类型攻击	攻击者将协议运行中某一类消息域替换成其他的消息域
密码分析	攻击者利用在协议运行中所获取的消息进行分析以获取有用的信息
证书操纵	攻击者选择或更改证书信息来攻击协议的运行
协议交互	攻击者选择新的协议和已知协议交互产生新的漏洞

1. 窃听

窃听是最基本的攻击方式，几乎所有的协议都通过加密解决窃听问题。窃听通常被看作被动攻击，因为攻击者并不影响合法用户的通信。除此之外的其他攻击方式都看作主动攻击。例如，明文传输认证信息的协议 POP3/SMTP、FTP、Telnet 都存在窃听的威胁。通常使用加密来保护敏感信息。