前　言

密码技术是网络空间安全的关键基础技术，与核技术、航天技术并称为“国家安全三大支撑技术”。密码作为国家重要战略资源，直接关系国家政治安全、经济安全、国防安全和信息安全。随着算力网络、云计算、物联网、车联网、智能电网、无线体域网等新型网络形态及网络服务的快速发展，数据安全和隐私保护问题日益成为学术界和产业界关注的焦点，对密码技术提出新挑战。近年来，针对新型网络环境的密码技术研究非常活跃，催生出抗合谋攻击的聚合签名、代理重签名、可搜索加密等新型密码体制，不仅丰富了密码学的理论基础，而且促进了密码技术在新型网络环境中的应用与发展。

本书围绕加密与签名技术展开，基于作者多年来在密码学和信息安全领域的研究成果，详细介绍面向新型网络环境的安全性更高、功能更全面、效率更优的密码方案。全书共 8 章，第 1 章介绍密码学的基础知识，主要包括密码学数学基础、哈希函数、公钥密码体制和数字签名等。第 2 章介绍强不可伪造的基于身份签名体制，主要包括标准模型下强不可伪造的基于身份签名方案的攻击方法及改进方案等。第 3 章介绍无证书签名体制，主要包括标准模型下强不可伪造的无证书签名方案、面向移动支付交易的无证书签名方案和基于无证书签名的物联网数据认证方案等。第 4 章介绍抗合谋攻击的无证书聚合签名体制，主要包括面向车载自组织网络的无证书聚合签名方案、基于无证书聚合签名的多方合同签署协议和面向无线医疗传感器网络的无证书聚合签名方案等。第 5 章介绍具有附加性质的代理重签名体制，主要包括部分盲代理重签名体制、可撤销的基于身份代理重签名体制、在线/离线门限代理重签名体制、服务器辅助验证代理重签名体制和基于代理重签名的云端跨域身份认证方案等。第 6 章介绍不可否认的强指定验证者签名体制，主要包括形式化模型、标准模型下不可否认的强指定验证者签名方案等。第 7 章介绍可搜索加密体制，主要包括支持策略隐藏且密文长度恒定的可搜索加密方案、基于云边协同的无证书多用户多关键词密文检索方案和基于无证书可搜索加密的 EHR 数据密文检索方案等。第 8 章介绍签密体制，主要包括基于多消息多接收者签密的医疗数据共享方案、基于签密和区块链的车联网电子证据共享方案和无线体域网中支持多密文等值测试的聚合签密方案等。

本书相关研究得到了国家密码科学基金项目(2025NCSF02040)、国家自然科学基金项目(62362059)、甘肃省高等学校产业支撑计划项目(2023CYZC-09)、甘肃省重点研发计划项目(23YFGA0081)、甘肃省自然科学基金重点项目(23JRRA685)、甘肃省基础研究创新群体项目(23JRRA684)和西北师范大学研究生培养质量提升-研究生一流教材建设项目的资助，感谢以上项目及西北师范大学、广州大学、密码科学技术全国重点实验室、丝绸之路信息港(甘肃)研究院有限责任公司、国网甘肃省电力公司电力科学研究院、甘肃海丰信息科技有限公司、甘肃创信信息科技有限责任公司和甘肃省商用密码行业协会的大力支持。特别感谢我的硕士研究生导师陆洪文教授、博士研究生导师王彩芬教授和博士后合作导师冯登国院士，是他们引领我走进充满挑战和激情的密码学研究领域。感谢杜小妮教授、冯涛教授、牛淑芬教授、张学军教授、陆军教授、贾俊杰副教授、曹天涯副教授、谢宗阳副教授、蓝才会副教授、姚海龙副教授和闫军才副研究员为本书的撰写提供了许多宝贵建议。此外，感谢研究生李松谕、魏丽珍、杨兰、李沐紫、罗熙来、王晨赓、李瑞婷、王雅琪、廉舒茜、姚恪、张园馨、钟亚彤、何君茹、王多加和周毅为本书的出版做了大量辅助性工作。

限于作者水平，书中难免存在不妥之处，恳请读者批评指正。

杨小东

2025 年 3 月定稿于兰州

目　录

前言
第 1 章　密码学基础 …… 1
1.1　密码学数学基础 …… 1
1.2　哈希函数 …… 3
1.3　公钥密码体制 …… 4
1.3.1　RSA 公钥密码 …… 5
1.3.2　ElGamal 公钥密码 …… 6
1.3.3　Diffie-Hellman 密钥交换协议 …… 6
1.4　数字签名 …… 8
1.4.1　RSA 数字签名 …… 8
1.4.2　ElGamal 数字签名 …… 9
参考文献 …… 9
第 2 章　强不可伪造的基于身份签名体制 …… 11
2.1　引言 …… 11
2.2　形式化模型 …… 12
2.3　标准模型下强不可伪造的基于身份签名方案 …… 13
2.3.1　Tsai 方案描述 …… 13
2.3.2　Tsai 方案的安全性证明 …… 14
2.3.3　Tsai 方案的安全性分析 …… 15
2.3.4　改进的基于身份签名方案 …… 17
2.4　可撤销和强不可伪造的基于身份签名方案 …… 20
2.4.1　Hung 方案描述 …… 21
2.4.2　Hung 方案的安全性分析 …… 22
2.4.3　改进的 RIBS 方案 …… 23
参考文献 …… 30
第 3 章　无证书签名体制 …… 33
3.1　引言 …… 33
3.2　形式化模型 …… 34
3.3　标准模型下强不可伪造的无证书签名方案 …… 36

3.3.1 Wu 方案描述 …… 36
3.3.2 Wu 方案的安全性分析 …… 38
3.3.3 改进的无证书签名方案 …… 39
3.4 面向移动支付交易的无证书签名方案 …… 45
3.4.1 Qiao 方案描述 …… 45
3.4.2 Qiao 方案的安全性分析 …… 46
3.4.3 改进的无双线性对的无证书签名方案 …… 47
3.5 基于无证书签名的物联网数据认证方案 …… 50
参考文献 …… 62
第 4 章 抗合谋攻击的无证书聚合签名体制 …… 65
4.1 引言 …… 65
4.2 无证书聚合签名方案的安全性定义 …… 67
4.3 面向车载自组织网络的无证书聚合签名方案 …… 69
4.3.1 Wang 方案描述 …… 69
4.3.2 Wang 方案的安全性分析 …… 70
4.3.3 面向 VANETs 的改进 CLAS 方案 …… 72
4.4 基于无证书聚合签名的多方合同签署协议 …… 78
4.4.1 Cao 方案描述 …… 78
4.4.2 Cao 方案的安全性分析 …… 80
4.4.3 面向多方合同签署的改进 CLAS 方案 …… 82
4.5 面向无线医疗传感器网络的无证书聚合签名方案 …… 84
4.5.1 Zhan 方案描述 …… 84
4.5.2 Zhan 方案的安全性分析 …… 87
4.5.3 面向无线医疗传感器网络的改进 CLAS 方案 …… 90
参考文献 …… 99
第 5 章 具有附加性质的代理重签名体制 …… 102
5.1 引言 …… 102
5.2 部分盲代理重签名体制 …… 104
5.2.1 形式化模型 …… 104
5.2.2 双向部分盲代理重签名方案 …… 106
5.3 可撤销的基于身份代理重签名体制 …… 111
5.3.1 形式化模型 …… 112
5.3.2 标准模型下可撤销的双向基于身份代理重签名方案 …… 114
5.4 在线/离线门限代理重签名体制 …… 121
5.4.1 变色龙哈希函数 …… 122

5.4.2　三种常用的密码协议 …… 123
5.4.3　形式化定义 …… 124
5.4.4　基于变色龙哈希函数的在线/离线门限代理重签名方案 …… 125
5.5　服务器辅助验证代理重签名体制 …… 129
5.5.1　形式化模型 …… 130
5.5.2　强不可伪造的服务器辅助验证代理重签名方案 …… 130
5.6　基于代理重签名的云端跨域身份认证方案 …… 134
5.6.1　跨域身份认证信任模型 …… 135
5.6.2　方案描述 …… 136
5.6.3　有效性分析 …… 143
5.6.4　其他性能分析 …… 146
参考文献 …… 147
第 6 章　不可否认的强指定验证者签名体制 …… 151
6.1　引言 …… 151
6.2　形式化模型 …… 152
6.3　标准模型下不可否认的强指定验证者签名方案 …… 155
参考文献 …… 162
第 7 章　可搜索加密体制 …… 164
7.1　引言 …… 164
7.2　形式化模型 …… 165
7.3　支持策略隐藏且密文长度恒定的可搜索加密方案 …… 167
7.4　基于云边协同的无证书多用户多关键词密文检索方案 …… 177
7.5　基于无证书可搜索加密的 EHR 数据密文检索方案 …… 184
7.5.1　系统模型 …… 184
7.5.2　方案描述 …… 185
7.5.3　安全性与性能分析 …… 190
参考文献 …… 192
第 8 章　签密体制 …… 195
8.1　引言 …… 195
8.2　形式化模型 …… 197
8.3　基于多消息多接收者签密的医疗数据共享方案 …… 199
8.4　基于签密和区块链的车联网电子证据共享方案 …… 205
8.5　无线体域网中支持多密文等值测试的聚合签密方案 …… 213
参考文献 …… 221

第 1 章　密码学基础

本章主要介绍密码学的一些基础知识，包括双线性映射、数学困难问题、哈希函数、公钥密码体制、数字签名等。这些知识对于读者阅读本书后面章节是非常必要的。

1.1　密码学数学基础

定义 1.1　设 F 是一个非空集合，$*$是一个二元运算，若 F 对于$*$满足如下四个性质，则称 F 是一个群[1]，记为 $(F,*)$。

(1) 封闭性：任取元素 $a,b\in F$，满足 $a*b\in F$。

(2) 结合律：任取元素 $a,b,c\in F$，有 $a*(b*c)=(a*b)*c$。

(3) 单位元：任取元素 $a\in F$，存在元素 $e\in F$，使得 $a*e=e*a=a$。

(4) 逆元：任取元素 $a\in F$，存在元素 $a^{-1}\in F$，使得 $a*a^{-1}=a^{-1}*a=e$。

如果群 F 包含的元素个数是有限的，那么称 F 为有限群；否则，称 F 为无限群。F 包含的元素个数称为 F 的阶，记为 $|F|$。若 $(F,*)$ 中的元素满足交换律，即任取元素 $a,b\in F$，满足 $a*b=b*a$，则称 F 是一个交换群[2]。

定义一个群中元素的幂运算为该元素的重复运算，即 $a^n=\underbrace{a+\cdots+a}_{n}$，规定 $a^0=e$。若对于元素 $a\in F$，存在正整数 $i\in Z$ 使得 $a^i=e$，则称满足此要求的最小正整数 i 为元素 a 的阶[3]。

若群 F 中的每个元素可以表示为一个元素 $a\in F$ 的幂 a^k，则称 F 是一个循环群，记为 $F=\langle a\rangle=\{a^k\mid k\in Z\}$，元素 a 被称为 F 的生成元。

定义 1.2　设 F 是一个非空集合，+和$*$是两个二元运算，若 F 对于+和$*$满足如下三个性质，则称 F 是一个域[4]，记为 $(F,+,*)$。

(1) $(F,+)$ 是一个交换群。

(2) $(F^*,*)$ 是一个交换群，这里 $F^*=F\setminus\{0\}$。

(3) 分配律：任取元素 $a,b,c\in F$，满足

$$a*(b+c)=a*b+a*c \quad 和 \quad (b+c)*a=b*a+c*a$$

若域 F 的元素个数是有限的，则称 F 为有限域；否则，称 F 为无限域[5]。

设 $q>3$ 是一个素数，集合 $Z_q=\{0,\cdots,q-1\}$ 对于模加法 $\oplus$ 和模乘法 $\otimes$ 构成一个有限域[6]，即任取元素 $a,b\in Z_q$，定义 $a\oplus b=a+b \bmod q$ 和 $a\otimes b=a\times b \mod q$，其中+和×分别是整数的普通加法和乘法。

令椭圆曲线 E 由满足方程 $y^2=x^3+ax+b \bmod q$ 的解 (x,y) 所对应的点构成，其中 $a,b\in Z_q$ 且 $4a^3+27b^2\neq 0 \bmod q$。一个基于 E 的椭圆曲线加法群定义为 $G=\{(x,y)\in E\mid x,y\in Z_q\}\bigcup\{O\}$，这里 O 是一个无穷远点；根据弦切(chord-and-tangent)法则[7]，G 中加法和倍乘运算分别定义为 $U=Q+R$ 和 $kR=\underbrace{R+\cdots+R}_{k}$，其中 $U,Q,R\in G$。关于椭圆曲线及其运算的详细介绍请参阅文献[8]～[10]。

定义 1.3 假设 G_1 和 G_2 是两个阶为素数 q 的乘法循环群，g 是 G_1 的一个生成元。如果映射 $e:G_1\times G_1\to G_2$ 满足以下三个性质，则称 e 是一个双线性映射或双线性对[11]。

(1) 双线性：对于任意 $x,y\in Z_q^*=Z_q\setminus\{0\}$，有 $e(g^x,g^y)=e(g,g)^{xy}$。

(2) 非退化性：$e(g,g)\neq 1_{G_2}$，其中 1_{G_2} 表示 G_2 中的单位元。

(3) 可计算性：对于 $x,y\in Z_q^*$，存在有效的算法计算 $e(g^x,g^y)$。

双线性映射是设计密码方案(如基于身份的密码方案)的重要工具，可以利用有限域上超椭圆曲线中的 Tate 对或 Weil 对来构造[12,13]。

可证明安全性理论在一定的安全模型下能够证明一个密码方案达到特定的安全目标，采用“归约”方法将密码方案的安全性关联到某个数学困难问题。由于数学困难问题是公认难以求解的，因此证明攻击者在多项式时间内攻破密码方案的概率是可忽略的。下面给出与本书密码方案相关的数学困难问题[14-16]，密码方案的安全性依赖于这些数学问题的困难性，即无法在多项式时间内以不可忽略的概率解决这些数学困难问题。

定义 1.4 大整数因子分解问题：给定一个大整数 $n=pq$，计算 n 的两个素数因子 p 和 q。

定义 1.5 离散对数(discrete logarithm，DL)问题：令 p 是一个大素数，Z_p^* 是一个乘法循环群，g 是 Z_p^* 的一个生成元。给定 Z_p^* 中的一个二元组 (g,y)，计算 x 使得 $y=g^x$。

定义 1.6 椭圆曲线离散对数(elliptic curve discrete logarithm，ECDL)问题：给定一个二元组 $(g,g^a)\in G_1^2$，其中 G_1 是一个椭圆曲线群，计算 $a\in Z_q^*$。

定义 1.7 计算性 Diffie-Hellman(computational Diffie-Hellman，CDH)问题：给定一个三元组 $(g,g^a,g^b)\in G_1^3$，其中 $a,b\in Z_q^*$ 是未知的，计算 $g^{ab}\in G_1$。

定义 1.8　判定性 Diffie-Hellman(decisional Diffie-Hellman，DDH)问题：给定一个四元组 $(g,g^a,g^b,g^c)\in G_1^3$，其中 $a,b,c\in Z_q^*$ 是未知的，判定 $c=ab \bmod q$ 是否成立。

定义 1.9　Diffie-Hellman 逆(Diffie-Hellman inversion，DHI)问题：给定一个二元组 $(g,g^a)\in G_1^2$，其中 $a\in Z_q^*$ 是未知的，计算 $g^{a^{-1}}\in G_1$。

定义 1.10　双线性 Diffie-Hellman(bilinear Diffie-Hellman，BDH)问题：给定一个四元组 $(g,g^a,g^b,g^c)\in G_1^3$，其中 $a,b,c\in Z_q^*$ 是未知的，计算 $e(g,g)^{abc}\in G_2$。

定义 1.11　判定双线性 Diffie-Hellman(decisional bilinear Diffie-Hellman，DBDH)问题：给定一个四元组 $(g,g^a,g^b,g^c)\in G_1^4$ 和一个元素 $Z\in G_2$，其中 $a,b,c\in Z_q^*$ 是未知的，判断 $Z=e(g,g)^{abc}$ 是否成立。

定义 1.12　平方 Diffie-Hellman(square Diffie-Hellman，SDH)问题：给定一个二元组 $(g,g^a)\in G_1^2$，其中 $a\in Z_p^*$ 是未知的，计算 $g^{a^2}\in G_1$。

定义 1.13　q-判定双线性 Diffie-Hellman 指数(q-decisional bilinear Diffie-Hellman exponent，q-BDHE)问题：给定 G_2 中的一个随机元素 T 和 G_1 中的一个元组 $y_{g,a,q}=(g_1,g_2,\cdots,g_q,g_{q+2},\cdots,g_{2q},g^r)\in G_1^{2q+1}$，其中 $a,r\in Z_p^*$ 未知且 $g_i=g^{a^i}$，判定 $(g,y_{g,a,q},e(g_{q+1},g^r))$ 与 $(g,y_{g,a,q},T)$ 是否相同。

定义 1.14　判定线性 Diffie-Hellman(decisional linear Diffie-Hellman，DLDH)问题：给定一个六元组 $(g_1,g_2,g_3,g_1^a,g_2^b,g_3^c)\in G_1^6$，其中 $a,b,c\in Z_q^*$ 是未知的，判定 $c=a+b \bmod q$ 是否成立。

1.2　哈 希 函 数

哈希(Hash)函数是密码学的基本工具，被广泛应用于数字签名、消息完整性验证、区块链等领域。Hash 函数是一种将任意长度的消息压缩成一个固定长度消息的函数，其输出值通常被称为 Hash 值(或哈希值)。Hash 函数的功能是为消息产生一个“数字指纹”，其长度通常为 128～512bit。Hash 函数通常又被称为单向散列函数、杂凑函数或消息摘要，在实际应用中通常采用特定的混合操作来设计 Hash 函数，而不是基于经典的数学困难问题。目前常用的哈希函数有消息摘要算法 MD5、安全散列算法 SHA-512、国密杂凑算法 SM3 等[15,16]。

定义 1.15　Hash 函数 $H:\{0,1\}^*\to\{0,1\}^l$ 是将一个任意长度的消息 m 映射为一个固定长度为 l、输出值 $h=H(m)$ 的函数，必须满足如下四个性质。

(1) 可计算性：给定消息 m，能够在多项式时间内计算哈希值 $h=H(m)$。

(2) 单向性：给定哈希值 $h=H(m)$，在多项式时间内计算 m 是不可行的。

(3) 弱碰撞性：给定一个消息 m_1，寻找另外一个消息 m_2，使得 $H(m_1)=H(m_2)$ 在计算上是不可行的。

(4) 强碰撞性：寻找两个不同的消息 m_1 和 m_2，使得 $H(m_1)=H(m_2)$ 在计算上是不可行的。

Hash 函数本质上是一个确定性算法，相同的输入消息对应相同的输出值(哈希值)。然而，固定长度的输出意味着所有输入输出组合中一定存在碰撞。例如，MD5 的抗碰撞性较差，无法有效抵抗生日攻击[15]。因此，一个安全的 Hash 函数需要满足以下条件：输入消息中任何一个比特的改变都会导致雪崩效应，产生一个完全不同的哈希值，攻击者很难找到有效的方法计算出哈希函数的碰撞。

如果一个哈希函数 H 满足以下三个性质，则认为 H 是一个随机预言机[16]。

(1) 均匀性：对于任意输入 m，对应的输出 $H(m)$ 在 $\{0,1\}^l$ 上是均匀分布的。

(2) 确定性：对于相同的输入 m，输出值 $H(m)$ 也是相同的。

(3) 有效性：对于输入的 m，能在有效时间内计算 $H(m)$。

1.3 公钥密码体制

密码学的基本安全目标主要包括保密性、完整性、可用性和不可抵赖性。其中，保密性主要确保信息仅被合法用户访问，而不能泄露给非授权用户。根据密钥方式，密码体制分为两大类：对称密码体制和非对称密码体制。对称密码体制又称单钥密码体制，解密密钥和加密密钥相同或从一个密钥很容易推导出另外一个密钥。常用的对称密码算法包括数据加密标准(DES)、三重数据加密算法(3DES)、高级加密标准(AES)、国际数据加密算法 (IDEA)、国密分组密码算法(SM4)、祖冲之算法(ZUC)等[17]。对称密码算法的优点是加密和解密的速度快，但存在密钥管理复杂、密钥分发需要安全信道、难以实现不可否认性等问题[18]。

公钥密码体制能够有效解决对称密码体制中的密钥分配和数字签名问题，在加密和解密阶段使用不同的密钥。在公钥密码体制中，每个用户拥有一个公开的公钥和秘密的私钥，私钥被用来签名或解密消息，对应的公钥来验证签名的合法性或加密消息。攻击者很难通过公钥计算出私钥，其难度等价于求解一个数学困难问题[19]。常用的公钥密码算法有国密公钥密码算法(SM2)、国密标识密码算法(SM9)、基于大整数因子分解问题的加密算法(RSA)、基于有限域离散对数问题的加密算法(ElGamal)、基于椭圆曲线离散对数问题的加密算法(ECC)等。

基于公钥密码体制的加密消息流程如图 1.1 所示。

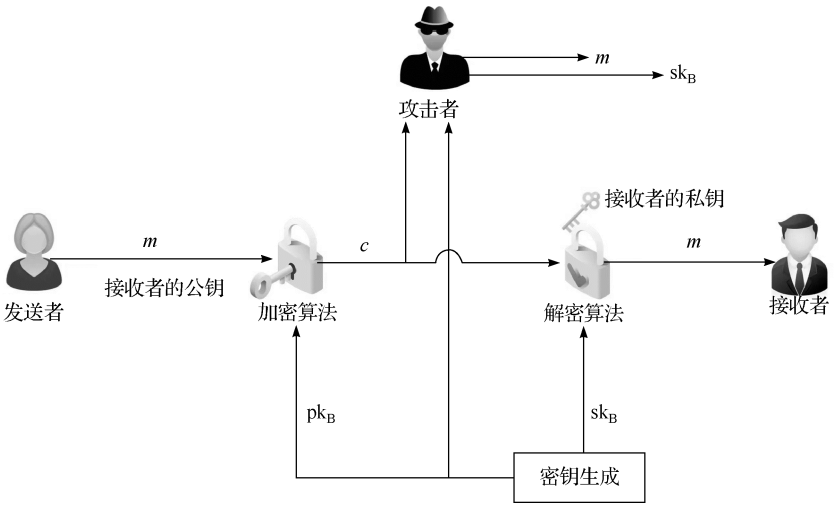

图 1.1　基于公钥密码体制的加密消息流程

假设消息的发送者和接收者分别为 Alice 和 Bob，Alice 利用 Bob 的公钥 $\mathrm{pk_B}$ 和加密算法 $\mathrm{Enc}(\cdot)$ 对消息 m 进行加密，生成对应的密文 $c=\mathrm{Enc}_{\mathrm{pk_B}}(m)$。Bob 使用自己的私钥 $\mathrm{sk_B}$ 和解密算法 $\mathrm{Dec}(\cdot)$ 对密文 c 进行解密，获得消息 $m=\mathrm{Dec}_{\mathrm{sk_B}}(c)$。

1.3.1　RSA 公钥密码

1976 年，Diffie 等[20]发表了 *New directions in cryptography*，提出了公钥密码体制的思想。1978 年，Rivest 等[21]提出了第一个公开的公钥密码方案 RSA，该方案成为目前使用最广泛的公钥密码体制之一，其安全性基于大整数因子分解问题。RSA 是一个确定性的加密方案，包括如下三个算法。

1. 密钥生成

(1) 选择两个秘密的大素数 p 和 q。

(2) 计算两个素数的乘积 $n=pq$ 和欧拉函数 $\phi(n)=(p-1)(q-1)$。

(3) 随机选择一个整数 $e(1<e<\phi(n))$，满足 e 和 $\phi(n)$ 互素，即 $\gcd(e,\phi(n))=1$。

(4) 计算 e 的逆元 $d=e^{-1} \bmod \phi(n)$。

(5) 保密私钥 d，公开公钥 (n,e)。

2. 加密

对于消息 m，发送者利用公钥 (n,e) 执行如下的加密操作：

$$c = m^e \bmod n$$

其中，c 为消息 m 的密文。

3. 解密

对于密文 c，接收者利用私钥 d 执行如下的解密操作来恢复消息：

$$m = c^d \bmod n$$

1.3.2 ElGamal 公钥密码

1985 年，ElGamal[22]提出了一种基于离散对数问题的公钥密码方案，通常称为 ElGamal 公钥密码体制。该方案是一个随机化的加密方案，密文依赖于明文和随机数，即同一个消息多次加密后得到的密文不一定相同。ElGamal 公钥密码方案主要包括如下三个算法。

1. 密钥生成

(1) 选择一个大素数 p，其中 p–1 有一个大素数因子。

(2) 选择 g 为有限群 Z_p^* 的一个生成元。

(3) 随机选择一个整数 $x(1 \leqslant x \leqslant p-2)$，计算 $y = g^x \bmod p$。

(4) 保密私钥 x，公开公钥 y。

2. 加密

对于消息 m，发送者利用公钥 y 执行如下的加密操作。

(1) 随机选择一个整数 $k(1 \leqslant k \leqslant p-2)$。

(2) 计算 $c_1 = g^k \bmod p$。

(3) 计算 $c_2 = y^k m \bmod p$。

(4) 设置密文 $c = (c_1, c_2)$。

3. 解密

对于密文 c，利用私钥 x 计算消息 $m = c_2 (c_1^x)^{-1} \bmod p$。

1.3.3 Diffie-Hellman 密钥交换协议

1976 年，Diffie 等[20]提出了一种在两个用户间进行密钥协商的协议，即 Diffie-Hellman 密钥交换协议，通信双方可以在不安全的公开信道上协商产生一个共享的秘密密钥。该协议的安全性基于有限群上的离散对数问题。这个密钥交换协议只能用于密钥的交换，不能进行消息的加密和解密。通信双方确定共同的

密钥后，需要使用其他对称加密算法实现消息的加密与解密。假设通信双方为 Alice 和 Bob，该协议的执行过程如图 1.2 所示，具体描述如下。

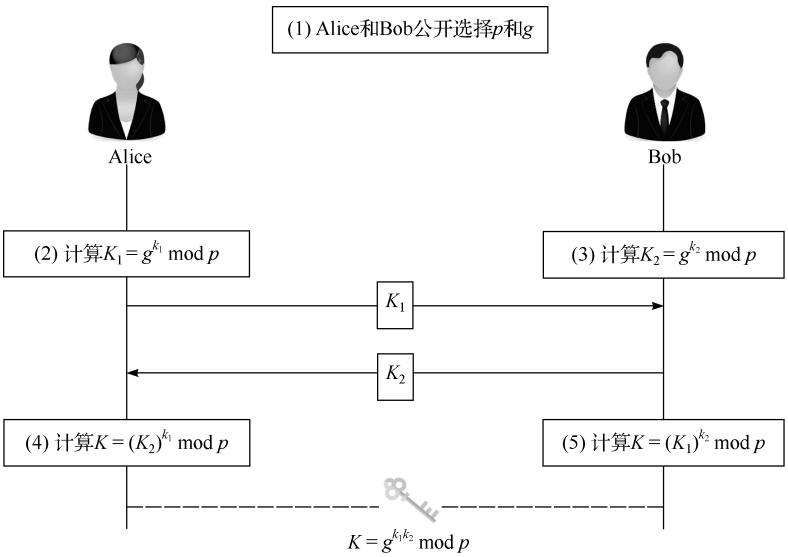

图 1.2　Diffie-Hellman 密钥交换协议的执行过程

1. 系统参数生成

Alice 和 Bob 共同产生如下的系统参数：

(1) 选择一个大素数 p，其中 $p-1$ 有一个大素数因子。

(2) 选择 g 为有限群 Z_p^* 的一个生成元。

(3) 公开系统参数 (p,g)。

2. 密钥协商

(1) Alice 随机选择一个整数 $k_1(1 \leqslant k_1 \leqslant p-2)$，计算 $K_1=g^{k_1} \bmod p$，然后发送 K_1 给 Bob。

(2) Bob 随机选择一个整数 $k_2(1 \leqslant k_2 \leqslant p-2)$，计算 $K_2=g^{k_2} \bmod p$，然后发送 K_2 给 Alice。

(3) Alice 计算共享密钥 $K=(K_2)^{k_1} \bmod p$。

(4) Bob 计算共享密钥 $K=(K_1)^{k_2} \bmod p$。

在上述密钥协商过程中，由于

$$K=(K_2)^{k_1} \bmod p=(g^{k_2} \bmod p)^{k_1} \bmod p=g^{k_2k_1} \bmod p=(g^{k_1} \bmod p)^{k_2}=(K_1)^{k_2} \bmod p$$

因此，Alice 和 Bob 能生成一个相同的密钥 K。然而，Diffie-Hellman 密钥交换协议无法抵抗中间人攻击，在实际应用中需要利用数字签名等认证机制解决中间人攻击问题[19]。

1.4 数 字 签 名

数字签名是公钥密码的重要组成部分，在数据完整性检验、身份鉴别、防否认等方面发挥着重要作用，已成为网络信息安全的关键技术之一。在数字签名中，公钥和私钥的顺序正好与公钥加密系统相反，发送者先利用自己的私钥生成消息的数字签名，当接收者收到数字签名和消息后，利用发送者的公钥验证这个数字签名的有效性。一方面，数字签名使接收者能验证发送者的签名，但不能伪造发送者的签名；另一方面，发送者不能否认所签发消息的有效签名。一旦收发双方发生争执时，由第三方仲裁者出面协商解决。第一个数字签名方案由 Rivest 等[21]提出，此后数字签名的理论与技术在密码学界受到广泛的重视。具有代表性的数字签名方案包括基于有限域离散对数问题的 ElGamal 签名方案[22]及其变形的相关签名方案[23,24]。

1.4.1 RSA 数字签名

RSA 密码方案[21]可以用于加密和数字签名，下面介绍 RSA 密码方案的签名功能。

1. 密钥生成

(1) 选择两个秘密的大素数 p 和 q。

(2) 计算两个素数的乘积 $n = pq$ 和欧拉函数 $\phi(n) = (p-1)(q-1)$。

(3) 随机选择一个整数 $e(1 < e < \phi(n))$，满足 e 和 $\phi(n)$ 互素，即 $\gcd(e, \phi(n)) = 1$。

(4) 计算 e 的逆元 $d = e^{-1} \bmod \phi(n)$。

(5) 保密私钥 d，公开 n 和公钥 e。

2. 签名

对于消息 m，签名者利用私钥 d 计算 m 的签名 $\sigma = m^d \bmod n$。

3. 验证

对于签名 σ，验证者利用公钥 e 验证等式 $m = \sigma^e \bmod n$ 是否成立。若等式成

立，则验证者接受 σ 是 m 的有效签名。

1.4.2　ElGamal 数字签名

ElGamal 数字签名方案[22]是一个非确定性的签名方案，其安全性基于离散对数问题的困难性。基于 ElGamal 数字签名方案的变体非常多，如美国数字签名标准(DSS)等。下面主要介绍 ElGamal 数字签名方案的签名功能。

1. 密钥生成

(1) 选择一个大素数 p，其中 p–1 有一个大素数因子。

(2) 选择 g 为有限群 Z_p^* 的一个生成元。

(3) 随机选择一个整数 $x(1 \leqslant x \leqslant p-2)$，计算 $y = g^x \bmod p$。

(4) 保密私钥 x，公开公钥 y。

2. 签名

对于消息 m，签名者利用私钥 x 执行如下的签名操作。

(1) 随机选择一个整数 $k(1 \leqslant k \leqslant p-2)$。

(2) 计算 $\sigma_1 = g^k \bmod p$。

(3) 计算 $\sigma_2 = (m-x)k^{-1} \bmod (p-1)$。

(4) 设置签名 $\sigma = (\sigma_1, \sigma_2)$。

3. 验证

对于消息 m 的签名 $\sigma = (\sigma_1, \sigma_2)$，验证者通过公钥 y 验证等式 $(\sigma_1)^{\sigma_2} y = g^m \bmod p$ 是否成立。若该等式成立，则验证者接受签名 σ。

参 考 文 献

[1] 王小云, 王明强, 孟宪萌, 等. 公钥密码学的数学基础[M]. 2 版.北京: 科学出版社, 2022.

[2] 陈恭亮. 信息安全数学基础[M]. 北京: 清华大学出版社, 2004.

[3] 许春香, 周俊辉. 信息安全数学基础[M]. 成都: 电子科技大学出版社, 2008.

[4] 杨波. 网络空间安全数学基础[M]. 北京: 清华大学出版社, 2020.

[5] 姜正涛. 信息安全数学基础[M]. 北京: 电子工业出版社, 2017.

[6] 任伟. 信息安全数学基础: 算法、应用与实践[M]. 2 版. 北京: 清华大学出版社, 2018.

[7] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48(177): 203-209.

[8] 李超, 付邵静. 信息安全数学基础[M]. 北京: 电子工业出版社, 2015.

[9] 巫玲. 信息安全数学基础[M]. 北京: 清华大学出版社, 2016.

[10] 常相茂. 信息安全数学基础[M]. 西安: 西安电子科技大学出版社, 2019.
[11] 裴定一, 徐祥, 董军武.信息安全数学基础[M]. 2 版. 北京: 人民邮电出版社, 2016.
[12] 秦艳琳. 信息安全数学基础[M]. 武汉: 武汉大学出版社, 2014.
[13] 旭云, 廖永建, 熊虎. 信息安全数学基础[M]. 2 版. 北京: 科学出版社, 2022.
[14] 贾春福, 钟安鸣, 赵源超. 信息安全数学基础[M]. 北京: 清华大学出版社, 2018.
[15] 周福才, 徐剑. 格理论与密码学[M]. 北京: 科学出版社, 2013.
[16] 李发根, 廖永建. 数字签密原理与技术[M]. 北京: 科学出版社, 2014.
[17] BEDOUI M, MESTIRI H, BOUALLEGUE B, et al. An improvement of both security and reliability for AES implementations[J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34(10): 9844-9851.
[18] 吴文玲, 眭晗, 张斌. 轻量级密码学[M]. 北京: 清华大学出版社, 2022.
[19] 杨波. 现代密码学[M]. 5 版. 北京: 清华大学出版社, 2022.
[20] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.
[21] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.
[22] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.
[23] SCHNORR C P. Efficient identification and signatures for smart cards[C]. Proceedings of Advances in Cryptology-CRYPTO'89, New York, USA, 1990: 239-252.
[24] 李雨潼. 基于身份及无证书签名方案的分析与研究[D]. 兰州: 西北师范大学, 2020.