公钥加密理论

薛 锐 著

科学出版社

公钥加密理论

薛 锐 著

本书出版得到以下项目资助:
中国科学院战略性先导科技专项(No. XDA06010701)
国家自然科学基金项目(No. 61170280; No. 61472414)

科 学 出 版 社

北 京

内 容 简 介

本书系统总结了典型的公钥加密方案和构造方法，从构建抗适应性选择密文攻击公钥加密方法的角度，分类介绍了标准模型下基于判定性和计算假设下的安全方案，随机应答器模型下从语义安全的方案到选择密文攻击下安全的典型方案转化方法，从身份加密、标签加密和广播加密到适应性选择密文攻击下安全方案转换方法，包含了迄今为止几乎所有抗适应性选择密文攻击的理论构造方法和格理论下典型的加密方案。书中介绍的实验序列、混合论证的方法和技术已经成为可证明安全密码学的基础。书中的论证全部采用实验序列的方式给出，有些是第一次出现，方便读者理解和掌握。本书同时介绍了目前学术界关注的部分公开研究问题。

本书可以作为信息安全专业研究人员的参考资料，为希望从事密码学和信息安全专业研究的本科高年级学生、研究生，尤其为希望从事可证明安全学习和研究的学者提供了丰富的参考内容。本书的内容将引导他们进入该领域的研究前沿。

图书在版编目(CIP)数据

公钥加密理论/薛锐著. —北京：科学出版社，2016.5

ISBN 978-7-03-048235-8

Ⅰ.①公… Ⅱ.①薛… Ⅲ.①公钥密码系统-研究 Ⅳ.①TN918.2

中国版本图书馆 CIP 数据核字(2016) 第 095493 号

责任编辑：孙伯元 高慧元 / 责任校对：桂伟利

责任印制：张 倩 / 封面设计：左 讯

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京通州皇家印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2016 年 6 月第 一 版 开本：720×1000 1/16

2016 年 6 月第一次印刷 印张：32 1/4

字数：631 000

定价：198.00 元

(如有印装质量问题，我社负责调换)

前　言

公钥密码学是现代密码学的一个分支, 它通过公钥密码手段解决实际或科学问题。它是现代密码学的一个非常年轻和活跃的研究领域, 其研究和应用范围正在持续扩张, 不断地超出人们的想象。公钥密码 (学) 是信息安全保障中使用的重要手段和工具。在现代密码学的发展为信息安全提供保障手段的同时, 信息安全保障的实际需要也刺激了公钥密码学的发展。

在 Diffie-Hellman (以及同一时期的 Merkle) 提出公钥密码学的思想后, 公钥密码学的发展可以用一日千里来形容。尤其是 Yao、Goldwasser、Micali、Shamir、Goldreich、Levin、Blum 和 Bellare 等众多计算机科学家和密码学专家, 成功地将现代密码学建立在计算复杂性的基础之上, 使其成为一门严格的科学分支。目前公钥加密系统衍生出众多的变形, 如身份加密 (identity based encryption)、属性加密 (attributive based encryption)、函数加密 (functional encryption) 等。对于不同类型的加密, 其安全性也根据实用环境的需要, 产生了各式各样的安全性定义。

本书主要集中介绍 "传统" 公钥加密方案的构造和证明方法, 即使用单个公钥进行加密, 使用相应单个私钥进行解密的方案。本书不包括上面提到的身份加密、属性加密等近年来出现的新型公钥加密方案。同时, 本书介绍的这些方案是在选择密文攻击下具有不可分辨加密, 就是常说的 IND-CCA 安全的加密方案。为了完整起见, 在基础知识部分介绍了一些选择明文攻击下安全 (CPA 安全) 的方案, 作为后文方案的基础。这里不涉及更高安全性的方案, 如选择打开安全的公钥加密方案等。这类安全性的概念在本书的最后一章中有所提及, 仅供参考。

书中囊括了迄今为止绝大多数典型的 CCA 安全的公钥加密方案, 并进行分类介绍。对于实用方案依照标准模型下的安全方案, 随机应答器模型下安全方案视不同的困难假设进行分类介绍。对于利用其他类型的加密方案, 比如身份加密方案, 构造的 CCA 安全公钥加密方案的方法以及理论性构造方法也分类单独介绍。这样做的目的是, 不同类型的读者可以集中阅读自己感兴趣的部分, 并且阅读完本书内容后就可以直接进入该专题研究前沿。另外, 理论构造框架是现代密码学重要组成部分, 故而单独成篇。对于格理论上的密码方案, 由于其知识基础的特殊性, 单独列在最后一篇。其中包括了作者近年来相关的研究工作。本书没有包括新近出现的利用不可分辨混淆 (indistinguishable obfuscation) 构建 CCA 安全的公钥方案, 主要原因

是这类构造不成熟, 某些方案中使用的混淆的类型可能不存在。有待进一步的探索。

为了使每个方案安全性证明条理清晰, 所有方案的证明均使用实验序列的方式给出, 为此作者对许多证明进行了改写。书中的基础知识部分讲解了公钥密码学中常用的证明技术。前 10 章可以作为密码学专业的学生教材使用。

本书内容既可以作为密码学与网络信息安全硕士研究生的学习内容, 又可以作为网络空间安全专业高年级本科学生的选学读物。本书的内容是自足的, 只要读者具有成熟的数学推理能力、大学本科的计算机和数学知识, 阅读本书就没有困难。本书内容可以视为 Katz 和 Lindell 所著的*Introduction to Modern Cryptography* 一书内容的继续和提高。

在本书写作过程中, 作者受到了中国科学院信息工程研究所和信息安全国家重点实验室的大力支持。尤其是得到了国家自然科学基金和中国科学院战略性先导科技专项 ——"面向感知中国的新一代信息技术研究" 课题的资助。谨表诚挚的谢意!

谢翔博士撰写了第 25~27 章的内容。常金勇博士撰写了第 9、10 章的内容。在此对他们表示衷心地感谢。本书其余内容均由作者使用 LaTeX 亲自书写完成, 其中几易其稿, 期间充分感受到使用 LaTeX 书写的便利, 所以要特别对 TeX 的发明人以及提供便利易用排版系统 CTex 的作者表示感谢。

许多专家对于本书的初稿提出了修改意见, 避免了很多笔误或谬误。蔡吉人院士、郑建华院士不仅指出了初稿的不足之处, 还提出了修改建议, 并且对于拙作提出了鼓励和期望。冯登国研究员仔细阅读书稿并形成了整整一笔记本修改意见和建议。其中不仅有题材选择方面的意见, 也有写作方面的体会, 甚至还有书名方面的思考, 使作者受益匪浅。尤其要感谢贾仃仃博士, 她在公钥密码方面深厚的造诣和敏锐的目光, 使我避免了很多的笔误。限于空间, 仅列举有过帮助的同行们姓名表示谢呈, 如果有遗漏敬请原谅。他们是 (按照姓氏拼音): 刘亚敏博士、路献辉博士、王欣、王学庆、徐静研究员、徐茂智教授、薛海洋博士、张仁军等。我的研究生韩春玲、丁珂兰、王欣、王贞灵等帮助准备了获图灵奖密码人物的简介。对于他们的帮助表示衷心的谢意。最后要对于我家人的理解、支持、帮助和鼓励表示感谢。

书中任何不足均是作者的责任。读者如果发现书中的缺点和疏漏, 请通过邮件: xuerui@iie.ac.cn 反馈给作者。在此表示感谢。

作　者

2015 年 11 月 9 日定稿于北京

术语和符号

英文术语	中文翻译
adaptive trapdoor function	适应性陷门函数
adaptively chosen ciphertext attack	适应性选择密文攻击
almost strongly universal hash family	几乎强通用摘要函数族
chosen plaintext attack	选择明文攻击
chosen-output security	选择输出安全
collusion threshold	合谋界值
correlated product	关联积
data encapsulation mechanism	数据封装机制
decisional composite residuosity assumption	判定复合剩余假设
detectable chosen ciphertext attack	可测选择密文攻击
dual lattice	对偶格
extractable hash proof system	可抽取摘要证明系统
gap decision assumption	间隙判定假设
identity based encryption	身份加密
key dependent message	关联密钥的消息
key encapsulation mechanism	密钥封装机制
leakage resilience security	容泄露安全性
lossy trapdoor function	亏值陷门函数
non-malleability	不可延展性
oblivious decryptors model	健忘解密模型
one-time message authentication code	一次性消息认证码
privately verifiability	可私密验证
publicly verifiability	可公开验证
randomness-related attack	相关随机串攻击
selective identity chosen ciphertext attack	选定身份的选择密文攻击
selective opening security	选择打开安全性
selective tag chosen ciphertext attack	选定标签的选择密文攻击
shortest vector problem	最短向量问题
tag-based encryption	标签加密
uniform ℓ-repetition distribution	均匀 ℓ 重复分布
unimodular matrix	幺模矩阵
universal hash proof system	通用摘要证明系统

符号	表达的意义
$\lceil x \rfloor_n$	简记 $x \mod n$。对任意 $x, n \in \mathbb{Z}^+$
$[n]$	表示集合 $\{1, \cdots, n\}$, 其中任意 $n \in \mathbb{Z}^+$
$\perp$	表示计算错误, 或者无效的结果, 甚至是不允许的行为
$a \perp b$	表示两个整数 a 和 b 互素
$x \leftarrow X$	表示在集合 X 中均匀随机选取一个元素 x
$x \leftarrow \mathcal{A}$	表示随机算法 $\mathcal{A}$ 输出值 x
$\mathrm{poly}(\cdot)$	表示某个固定的多项式
λ	本书使用 λ 表示安全参数
$a\,b$	表示比特串 $a \in \{0,1\}^*$ 和 $b \in \{0,1\}^*$ 接连而成的串
$a \vert b$	表示比特串的接连。与 $a\,b$ 互用
$\Pr[A \mid B]$	表示在条件 B 发生的条件下 A 发生的概率
$\Pr[A : B]$	表示在条件 A 发生前提下 B 发生的概率
$\mathbb{Z}_N$	表示模 N 的剩余类环
$\mathbb{Z}_N^*$	表示环 $\mathbb{Z}_N$ 中关于乘法的可逆元的全体
$\mathcal{QR}_N$	表示 $\mathbb{Z}_N$ 中关于乘法的平方剩余类的集合
$\mathcal{QR}_N^{\mathrm{abs}}$	表示 $\mathbb{Z}_N$ 的对称表达中平方数绝对值的集合

目　录

第二篇　标准假设下 CCA 安全方案

第三篇　随机应答器模型下的方案

第四篇　基于特定类方案的构造

第五篇　理论构造框架

第六篇　格理论上的构造

第一篇　公钥密码基础

第 1 章　公钥密码入门

1.1　公钥密码系统和安全性定义

1.1.1　公钥密码学初步

现代密码学是计算机科学、信息论和数学等学科紧密结合的一门学科。某种意义上说, 现代密码学诞生于 Shannon[1, 2] 的经典著作, 之前可以称为密码技术或古典密码学。现代密码学早期的技术发展, 更多的是受人们兴趣的驱动。一些有兴趣的人和有才华的人, 对于这门技术进行钻研, 设计一套加密方法或仪器。其他的人会通过自己的钻研, 利用个人的聪明才智进行破译攻击。如果破译成功, 则需要对原有的方法进行改进。如此反复, 进行技术革新。从这个意义上说, 之前的密码技术更具有艺术性、技巧性, 而非科学性。而以 Shannon 著作作为起点的现代密码学, 以坚实的数学和计算机科学理论为基础, 逐渐形成了一门严谨的科学。尽管在这门科学中, 依然存在着许多人为的假设和设计理念, 但它已经毫无疑问地、坚实地屹立于科学之林。而这些人为的假设正是需要人们今后证明或证伪的难题。

现代密码学的一个主要的特征是, 以数学、信息论等科学的手段进行严格的刻画, 以区别于古典密码学的人为艺术的构造和破解过程。现代密码学有别于古典密码学的方面在于: 对于密码学的各个方面都有了科学的描述和刻画。例如, 现代密码学的几乎所有方案, 都是以单向函数存在为前提的。许多方案的存在与单向函数的存在性是等价的。现代密码学研究对象的安全性, 方案构造的基础假设, 以及研究对象安全性的证明各个方面, 都有着严格精准的数学描述、刻画和证明过程。

如果现代密码学以 Shannon 的工作为标志, 公钥密码学则始于 Diffie 等[3] 的开山之作: *New directions in cryptography*。这篇经典文章, 突破了传统密码学中加密者与解密者必须共享相同密钥的思想。首次明确地提出, 加密密钥和解密密钥可以不同, 并且从加密密钥无法计算出解密密钥。加密密钥可以公开, 而只需要保密解密密钥。从公开密钥难以推导出相应的保密私钥。这就形成了公开密钥密码学, 简称为公钥密码学。

利用这个思想, Diffie 等成功地解决了密钥协商和建立的难题。设计出著名