本书获得河南省高等学校青年骨干教师资助计划项目（2015GGJS-001）、
河南省高等学校重点科研项目(19A413004)资助

基于格的公钥密码算法的分析与设计

孙 华 ◎ 著

科学技术文献出版社
SCIENTIFIC AND TECHNICAL DOCUMENTATION PRESS

基于格的公钥密码算法的分析与设计

孙 华◎著

科学技术文献出版社
SCIENTIFIC AND TECHNICAL DOCUMENTATION PRESS
·北京·

图书在版编目（CIP）数据

基于格的公钥密码算法的分析与设计 / 孙华著. —北京：科学技术文献出版社，2019.2
ISBN 978-7-5189-5072-0

Ⅰ.①基… Ⅱ.①孙… Ⅲ.①公钥密码系统—密码算法—研究 Ⅳ.①TN918.4

中国版本图书馆 CIP 数据核字（2018）第 280345 号

基于格的公钥密码算法的分析与设计

策划编辑：张 丹　　责任编辑：赵 斌　　责任校对：张吲哚　　责任出版：张志平

出 版 者　科学技术文献出版社
地　　址　北京市复兴路15号　邮编 100038
编 务 部　(010) 58882938，58882087（传真）
发 行 部　(010) 58882868，58882870（传真）
邮 购 部　(010) 58882873
官方网址　www.stdp.com.cn
发 行 者　科学技术文献出版社发行　全国各地新华书店经销
印 刷 者　北京虎彩文化传播有限公司
版　　次　2019 年 2 月第 1 版　2019 年 2 月第 1 次印刷
开　　本　710×1000　1/16
字　　数　153千
印　　张　8.75
书　　号　ISBN 978-7-5189-5072-0
定　　价　38.00元

前　言

随着计算机网络及通信技术的飞速发展，人们之间的信息交流呈现出国际化、网络化、数字化、智能化、宽带化的趋势，人类已经进入了信息时代。信息时代的主要特征是信息成了社会中最重要的一种资源和财富，信息的交流和处理手段成了人们生活中必不可少的部分。通过网络传输或获取信息，已从军事、政治、外交等重要领域日益普及到人们日常生活的各个领域。然而，信息技术是一把“双刃剑”，它一方面给人类带来了巨大的好处，另一方面又给人类带来了前所未有的威胁。如何保障信息在网络传输过程中不受各种干扰破坏或不发生泄露，保证信息安全，已成为当今信息时代的一个重要问题。

信息安全是一个综合性的交叉学科，它涉及数学、密码学、计算机科学、通信、控制、人工智能等诸多学科。信息安全的任务就是要采取技术手段及有效管理保护信息和信息系统免遭偶然或有意的非授权泄露、修改、破坏或丧失处理信息能力，实质是保护信息的安全性，即机密性、完整性、可用性、可控性和不可伪造性。保障信息安全的核心是密码技术，信息安全是密码学研究与发展的目的。

在量子计算时代，传统的密码体制将不再安全。如何应对量子计算机所带来的安全威胁，并设计出抗量子计算攻击的密码体制是人们不断追寻的目标，而格密码是该研究领域中最受关注的一个。目前，基于格上困难问题进行格密码体制的分析与设计已成为后量子密码研究中的重要内容。此外，利用破解格上困难问题的算法进行密码体制的安全性分析，已成为一种重要的手段。对格密码进行研究与应用，不仅具有重要的理论与实际意义，同时也是后量子时代密码学的研究热点。

根据密钥的产生方式，可将密码体制分为非对称密码和对称密码，即私钥密码体制和公钥密码体制。公钥密码体制为密码学的发展提供了新的理论和技术基础，一方面，公钥密码算法的基本工具不再是代换和置换，而是数学函数；另一方面，公钥密码算法中两个密钥的使用对保密性、认证、密钥分配等都有着深刻

的意义。数字签名是针对电子文档的一种签名确认技术，它由公钥密码发展而来，在信息安全，包括身份认证、数据完整性、不可否认性及匿名性等方面，特别是在大型网络安全通信中的密钥分配、认证及电子商务系统中具有重要作用。面对现实环境中许多特殊功能的需求，具有附加性质的数字签名算法不断涌现出来，并应用到不同的领域。签密是将机密性和不可伪造性合二为一的一种新的密码原语，是指能够在一个单一的逻辑步骤内同时实现加密和签名两种操作。该概念一经提出即吸引了广大的研究人员和学者，目前国内外不少研究人员已在该领域进行了广泛的研究和探索，不断推动着其研究向前发展。

本书内容分为三部分：第一部分介绍密码学的基础知识、格密码和可证明安全性理论；第二部分介绍基于格的数字签名及具有附件性质的签名方案；第三部分介绍签密技术及基于格的签密方案。本书作为基于格的公钥密码算法的分析与研究的一部专业著作，是笔者近年来从事基于格的公钥密码研究的相关成果总结，它不仅可以作为信息安全、计算机、通信工程等专业高年级本科生和研究生的教材与参考读物，也可供从事相关理论研究的技术人员参考使用。

在本书撰写过程中，安阳师范学院计算机与信息工程学院的领导和老师给予了大力支持，他们付出了大量的劳动，在此衷心地表示感谢。此外，笔者参阅了大量的相关图书和资料，并通过网络获取了很多资源，在此向各位原著作者一并表示致敬和感谢！由于笔者水平有限，书中难免存在不妥和错误之处，恳请各位专家和读者批评指正。

本书的相关工作得到了河南省高等学校青年骨干教师资助计划项目（2015GGJS-001）、河南省高等学校重点科研项目（19A413004）资助。

目　录

第 1 章

数学知识

密码学以数学理论为基础，涉及数论、代数结构、复杂性理论等，它们是设计密码算法和协议不可或缺的有力工具。本章主要介绍本书需要用到的数论、代数结构和复杂性理论，为后面密码学的学习做好准备，更多内容请参见参考文献［1-15］。

1.1 初等数论

数论是主要研究整数性质的一个重要的数学分支，它不仅仅是一门纯粹的数学学科，也是一门应用性很强的数学学科。如今，数论已广泛应用于通信、信息安全、电子等领域，尤其是在密码学方面涉及许多数论方法与技术。限于篇幅，本节仅简单介绍密码学中常用的一些数论中的基本概念和结论。

1.1.1 整除

通常用 $\mathbb{Z}$ 表示全体整数的集合，用 $\mathbb{N}$ 表示全体自然数的集合，下面给出整除的定义。

定义 1-1 给定两个整数 a，$b \in \mathbb{Z}$，如果存在整数 $q \in \mathbb{Z}$，使得 $a = bq$，那么就称 a 可被 b 整除，或者称 b 是 a 的因子，记作 $b \mid a$；反之，则说 a 不可被 b 整除，记作 $b \nmid a$。

设 a，b，$c \in \mathbb{Z}$，根据定义和乘法运算规律，可知整除有以下性质。

① 若 $a \mid b$，$b \mid c$，则 $a \mid c$。

② 若 $a \mid b$，$a \mid c$，则对于任意 x，$y \in \mathbb{Z}$，有 $a \mid bx + cy$。

③ 若 $a \mid b$，$b \mid a$，则 $a = \pm b$。

④ 若 $b \neq 0$，$a \mid b$，则 $|a| \leqslant |b|$。

定义 1-2 如果整数 $p > 1$ 且仅能被 1 和它本身整除，则称 p 为素数（也称为质数）。

在一般情况下，素数只取正数，若整数 $n > 1$ 且不是素数，则称为合数。

1.1.2 最大公约数

定义 1-3 设 a，b 是不全为 0 的整数，能同时整除 a 和 b 的最大正整数 d 称为最大公约数，记作 $d = \gcd(a, b)$。

根据定义可知，最大公约数 $d = \gcd(a, b)$，满足以下性质。

① 对于任意整数 x，均有 $\gcd(a, b) = \gcd(a, b + ax)$。

② 对于任意整数 x 和 y，均有 $d \mid ax + by$。

③ 若 $c \mid a$，$c \mid b$，则 $c \mid d$。

定义 1-4 设 a、b 是两个整数，如果 $\gcd(a, b) = 1$，则称它们互素。

关于最大公约数，我们有以下结论：

定理 1-1 若 $\gcd(x, a) = 1$，则有 $\gcd(x, ab) = \gcd(x, b)$。

定理 1-2 若 $\gcd(x, a) = 1$，$x \mid ab$，则 $x \mid b$。

1.1.3 同余及剩余类

定义 1-5 给定两个整数 a 和 b，如果它们除以 n 具有相同的最小非负余数，则称它们模 n 同余，记作 $a \equiv b(\mathrm{mod}n)$。显然，$a$ 和 b 模 n 同余等价于 $n \mid a - b$。

根据定义 1-5 可知，同余关系是一个等价关系，具有以下性质。

① 自反性：对于任意整数，$a \equiv a(\mathrm{mod}n)$。

② 对称性：若 $a \equiv b(\mathrm{mod}n)$，则 $b \equiv a(\mathrm{mod}n)$。

③ 传递性：若 $a \equiv b(\mathrm{mod}n)$，$b \equiv c(\mathrm{mod}n)$，则 $a \equiv c(\mathrm{mod}n)$。

不难证明，同余运算还满足如下性质。

① 若 $a \equiv b(\mathrm{mod}n)$，$c \equiv d(\mathrm{mod}n)$，则 $a \pm c \equiv b \pm d(\mathrm{mod}n)$。

② 若 $a \equiv b(\mathrm{mod}n)$，$c \equiv d(\mathrm{mod}n)$，则 $ac \equiv bd(\mathrm{mod}n)$。

③ 若 $ac \equiv bc(\mathrm{mod}n)$，$\gcd(c, n) = 1$，则 $a \equiv b(\mathrm{mod}n)$。

定理 1-3　若整数 $n \geqslant 1$，$\gcd(a, n) = 1$，则存在一个小于 n 的整数 c，使得 $ac \equiv 1(\mathrm{mod}n)$，称 c 为 a 模 n 的乘法逆元，记作 a^{-1}。

定义 1-6　在模 n 的运算中，将除以 n 同余的所有整数形成的集合称为模 n 的一个剩余类。

模 n 的剩余类有 n 个，n 个剩余类的 n 个代表元（每个代表元对应一个剩余类）构成一个模 n 的完全剩余类，记作 $\mathbb{Z}_n$。

定义 1-7　在模 n 的一个剩余类中，若有一个数与 n 互素，则该剩余类中所有元素均与 n 互素，并称该剩余类为既约剩余类。在模 n 的每个既约剩余类中取一个代表元，则它们组成一个既约剩余系，记作 $\mathbb{Z}_n^*$。

1.1.4　欧拉函数

定义 1-8　对于任意 $x \in \mathbb{N}$ 且 $x \geqslant 1$，令 $\Phi(x)$ 为小于 x 且与 x 互素的非负整数的个数，则称 $\Phi(x)$ 为欧拉函数。

根据定义 1-8 可知，欧拉函数具有以下性质。

① $\Phi(1) = 1$。

② 若 p 是素数，则 $\Phi(p) = p - 1$。

③ 若 $\gcd(a, b) = 1$，则 $\Phi(ab) = \Phi(a)\Phi(b)$。

定理 1-4　（欧拉定理）若 $\gcd(a, n) = 1$，则 $a^{\Phi(n)} \equiv 1\mathrm{mod}n$。

定理 1-5　（费尔马定理）若 p 为素数且 $\gcd(a, p) = 1$，则 $a^{p-1} \equiv 1\mathrm{mod}p$。

定义 1-9　给定素数 p，若存在一个整数 a，使得 $a\mathrm{mod}p$，$a^2\mathrm{mod}p$，…，$a^{p-1}\mathrm{mod}p$ 是各不相同的整数，并且组成模 p 的从 1 到 $p - 1$ 的一个既约剩余系，则称 a 为素数 p 的生成元。

1.1.5　同余方程

定理 1-6　（中国剩余定理）设 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数，令 $m = m_1 m_2 \cdots m_k$，$M_i = \dfrac{m}{m_i}$，那么，对于任意整数 $a_1, a_2, \cdots, a_k$，同余方程组 $x \equiv a_i(\mathrm{mod}m_i)$，其中，$1 \leqslant i \leqslant k$，有唯一解。该解是 $x \equiv M_1 M_1^{-1} a_1 + \cdots + M_k M_k^{-1} a_k(\mathrm{mod}m)$，其中，$M_i M_i^{-1} \equiv 1(\mathrm{mod}m_i)$。

定义 1-10　设整数 $n > 1$，$\gcd(a, n) = 1$，若同余方程 $x^2 \equiv a(\mathrm{mod}n)$ 有解，

则称 a 为模 n 的二次剩余；否则，称 a 为模 n 的二次非剩余。

1.2 代数结构

1.2.1 群

定义 1-11 设 G 是一个非空集合，在 G 上定义了一个二元运算“$\cdot$”，若满足以下条件，则将满足条件的集合 G 称为群，记作 $(G, \cdot)$。

① 运算封闭性成立，对于任意 $a, b \in G$，有 $a \cdot b \in G$。

② 结合律成立，对于任意 $a, b, c \in G$，有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$。

③ G 中存在一个元素 e，对于任意 $a \in G$，有 $a \cdot e = e \cdot a = a$，该元素称为 G 的单位元；

④ 对于任意 $a \in G$，存在一个元素 $a^{-1} \in G$，使得 $a \cdot a^{-1} = a^{-1} \cdot a = e$，该元素称为 a 的逆元。

如果对于群 G 中任意元素 $a, b \in G$，有 $a \cdot b = b \cdot a$，则称 G 为交换群或 Abel 群。

上述定义中，G 的运算“$\cdot$”指代一般意义下的运算，它可以是通常的乘法或加法。

定义 1-12 若群中元素的个数有限，称这个群为有限群；否则，称这个群为无限群。有限群中元素的个数称为群的阶，记作 $|G|$。

定义 1-13 如果群 G 中的每一个元素都是某个元素 $a \in G$ 的幂 a^k（k 为整数），则称 G 是一个循环群，a 称为 G 的一个生成元。

1.2.2 环

定义 1-14 设 R 是一个非空集合，在其上定义了两个二元运算“+”（加法）和“$\cdot$”（乘法），如果这些运算满足以下条件，那么就称 $(R, +, \cdot)$ 为一个环，记作 R。

① $(R, +)$ 是一个交换群。

② 乘法运算满足结合律，即对所有的 $a, b, c \in R$，有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$。

③ 乘法对加法满足分配律，即对所有的 a，b，$c \in R$，有 $a \cdot (b+c) = a \cdot b + a \cdot c$，$(b+c) \cdot a = b \cdot a + c \cdot a$。

如果一个环 R 还满足条件：对于任意 a，$b \in R$，有 $a \cdot b = b \cdot a$，则称其为交换环。同群一样，元素个数有限的环，称为有限环，否则，称为无限环。

定义 1-15　若对于环 R 中任意一个元素 a，都有 $ae = ea = a$，则称 e 为环 R 的单位元。如果环含有单位元，则单位元唯一。

定义 1-16　若含有单位元的环 R 存在一个非零元素 a^{-1}，有 $aa^{-1} = a^{-1}a = e$，称 a^{-1} 为 a 的逆元。

1.2.3　域

定义 1-17　设 F 是至少含有两个元素的集合，在其上定义了两个二元运算“+”（加法）和“·”（乘法），如果这些运算满足以下条件，那么就称集合 F 为域，记作 $(F, +, \cdot)$。

① F 的元素关于运算“+”构成交换群，其单位元为“0”。

② F 关于运算“·”构成交换群，其中，每一个非零元素 a 有一个逆元 a^{-1}。

③ 对于任意 a，b，$c \in F$，分配律成立，即 $(a+b) \cdot c = a \cdot c + b \cdot c$。

如果一个域包含的元素是有限的，则称为有限域，否则，称为无限域。有限域中所含元素的个数称为有限域的阶。

定理 1-7　有限域的阶一定是素数的幂。

定理 1-8　给定任意素数 p 和正整数 n，存在阶为 p^n 的有限域，记作 $\mathrm{GF}(p^n)$。

密码学中应用到的域一般是有限域，有限域又被称为 Galois 域，并以 $\mathrm{GF}(p^n)$ 表示，其中，p^n 表示有限域的阶。

定义 1-18　设 F_1、F_2 是两个域，称 F_1 到 F_2 的一个可逆映射 σ 为一个同构（映射），如果 σ 是保持运算的映射，即对于任意的 a，$b \in F_1$，有 $\sigma(a+b) = \sigma(a) + \sigma(b)$，$\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$。

1.3　计算复杂性理论

复杂性理论和密码学之间有着紧密的联系。计算复杂性理论是现代密码学的理论基础，也是构造安全密码体制的理论依据。密码学是复杂性理论的一个重要

应用领域，密码学的不断发展促进了复杂性理论的进一步深入研究。问题复杂性和算法复杂性是现代密码学中有关复杂性理论的两个主要内容，是密码分析技术中分析计算需求和破译密码固有难度的基础，为分析不同密码算法和技术的计算复杂性提供了有效工具。

计算复杂性理论给出了求解一个问题的计算是“容易”还是“困难”的确切定义，进而对问题和算法的复杂性加以分类。计算复杂性理论为密码体制的安全性提供了一种有效的描述方法：把破解密码体制的复杂度与解决某个已知问题的复杂度联系起来，从而把此密码体制的安全性归约为求解该问题的困难性。这一理论对现代密码学的发展起着重要作用。

1.3.1 问题与算法的复杂性

问题是指有待回答的一般性陈述或提问，常包括若干未知参数或自由变量。一个问题的描述由两部分组成：① 对其所有参数的一般性描述；② 说明其“答案”或“解”应具有的特性。给定问题所有未知参数的一组确定值后所对应的问题称为该问题的一个例子。

在诸多实际问题中，有一类问题其答案只有“是”或“非”两种可能，称之为判定问题。一个判定问题 D 可由它的所有例子构成的集 I 和 I 中那些答案为“是”的例子构成的集 I^+ 来表示，记作 $D=(I, I^+)$。通常 D 的一个例子可用一组参数值 θ 表示，因此，可将 I 和 I^+ 视为数集或数组集。实际中的绝大多数问题都可直接或间接地转化为判定问题。

设 c 为 D 的一个编码，由于问题的复杂度可能因为选择的编码方式不同而发生不同数量级的变化。因此，一个合理的编码应满足下列两个基本要求：① 编码是容易实现的；② 求解问题 D 的任意一个例子 θ 的计算复杂性与 $|c(\theta)|$ 有某种正比关系。

算法是一个关于某种运算规则的有限有序集合，这些规则确定了求解某一问题的一个运算序列。对该问题的任何例子，它能一步一步地执行计算。称一个算法可解某个计算问题是指这个算法可应用于这个问题的任何例子，并求得其解答。称一个问题是可解的，是指至少存在一个算法可解这个问题，否则就称该问题是不可解的。

一个算法的复杂性或有效性可以由执行该算法所需的运行时间和存储空间来度量，但在密码学应用中，人们更关心的是产生最终答案前算法所花费的时间。

因此，我们只研究算法的时间复杂度。由于一个算法的时间复杂度随着选用的计算机语言、用这一语言编写程序的方法及计算所用的计算机等因素的不同而有很大的差异，因此，在计算复杂性理论研究中，人们都采用统一的计算模型——图灵机。

1.3.2　算法与图灵机

图灵机是由英国数学家图灵在 1936 年首先提出的，至今仍被广泛应用于计算复杂性的理论研究中。下面介绍图灵机的基本模型。

图灵机的基本模型由一条输入带、一个读写头和一个有限控制器组成。输入带是半无限长的，它有无穷多个单元，每个单元可存放一个符号。有限控制器可控制读写头的左右移动。图灵机的一个基本动作可描述如下。

① 读写头读入所扫描单元的符号。

② 更新有限控制器的状态。

③ 读写头在扫描的单元上写入一个符号。

④ 读写头左移一单元，或者右移一单元，或者不移动。

严格地说，一台图灵机是一个七元组 $M=(Q, \sum, \Gamma, \delta, q_0, B, F)$，其中：

① Q 是状态集，它是一个非空有限集合。

② $\sum$ 是输入字母表，$\sum \subseteq \Gamma$，$B \notin \sum$。

③ Γ 是输入带符号集，它是一个非空有限集合。

④ B 是空白符，$B \in \Gamma$。

⑤ q_0 是初始状态，$q_0 \in Q$。

⑥ F 是终止状态集，$F \subseteq Q$。

⑦ δ 是转移函数，它是 $(Q-F)\times\Gamma$ 的某个子集到 $Q\times\Gamma\times\{L, R, S\}$ 的映射，L 表示左移一单元，R 表示右移一单元，S 表示不移动。如果一台图灵机的 δ 是单值的，则该图灵机是确定型图灵机；如果 δ 是多值的，则是非确定型图灵机。

一个算法的实现需要借助一定的计算模型。邱奇-图灵命题指出，如果一个算法在某个合理的计算模型上是可计算的，那么它在图灵机上也是可计算的。如果一个问题的规模为 n，则求解这个问题的算法所需的时间为 $T(n)$，它是 n 的函数。$T(n)$ 就是这个算法的时间复杂度，当输入规模 n 逐渐加大时，时间复杂度

的极限情形就是这个算法的渐近时间复杂度。

如果算法的时间复杂度为 $T(n)=O(n^k)$，其中，n 为规模，k 为常数，则该算法为多项式时间算法。如果 $k=0$，则算法是常数的；如果 $k=1$，则算法是线性的；如果 $k=2$，则算法是二次的。依此类推。

如果算法的时间复杂度为 $T(n)=O(k^{f(n)})$，其中，k 为大于 1 的常数，$f(n)$ 是规模 n 的多项式函数，如 $f(n)=n$，则该算法为指数时间算法。

如果算法的时间复杂度为 $T(n)=O(k^{f(n)})$，其中，k 为大于 1 的常数，$f(n)$ 大于常数而小于线性函数，如 $f(n)=\sqrt{n}$，则该算法为亚指数时间算法。

现在普遍接受的观点是：认为多项式时间算法是“好的算法”，是有效的算法，因此，称有多项式时间算法的问题是“易解的”，而不存在多项式时间算法的问题，则称它为“难解的”。

1.3.3 问题的复杂性分类

对于一个具体问题，其计算的复杂度就是指可解该问题的算法的计算复杂度。由于可解该问题的算法可能有若干种，通常将可解该问题的最有效算法的复杂度定义为该问题的计算复杂度。根据问题的复杂度程度，可将问题的计算复杂度大致分为 3 类：P 问题、NP 问题和 NP 完全问题。

P 问题：指所有可以在多项式时间内求解的问题，或者说在确定型图灵机求解该问题时有多项式时间算法。

NP 问题：指所有可以在多项式时间内验证的问题，或者说在非确定型图灵机求解该问题时有多项式时间算法。

显然，$P \subseteq NP$，但是“$P=NP$ 是否成立”，仍然是当代数学和理论计算机科学中最大的难题之一。

研究表明，在 *NP* 类中有一小类问题，利用确定型图灵机求解时没有多项式时间算法，不过，如果其中一个问题利用确定型图灵机求解时有多项式时间算法，那么 $P=NP$。这一小类问题就是 *NP* 完全问题。可以看出，*NP* 完全问题是 *NP* 类问题中一类最难的问题。

计算复杂性理论在密码学研究领域起到十分重要的作用。密码学中的安全性分为理论安全性和计算安全性，计算安全性就是基于 *NP* 难问题的。目前的公钥密码体制就是计算安全的，也就是说，公钥密码体制的安全性是基于某种难解问题的假设。