现代数学基础丛书 104

椭圆与超椭圆曲线公钥密码的理论与实现

王学理　裴定一 著

科学出版社
www.sciencep.com

中国科学院科学出版基金资助出版

现代数学基础丛书 104

椭圆与超椭圆曲线公钥密码的理论与实现

王学理 裴定一 著

科学出版社
北京

内 容 简 介

本书论述了椭圆与超椭圆曲线公钥密码学的基本理论及实现，其中包括：椭圆曲线公钥密码体制介绍，椭圆和超椭圆曲线的基本理论，定义在有限域上椭圆和超椭圆曲线的有理点的计数，椭圆和超椭圆曲线上的离散对数，椭圆和超椭圆曲线离散对数的初等攻击方法、指标攻击方法、代数几何攻击方法及代数数论攻击方法. 本书的特点之一，内容涉及面广，在有限的篇幅内，包含了必要的预备知识和较完备的数学证明，尽可能形成一个完整的体系；特点之二，用较为系统和统一的方法总结了大部分有限域上椭圆和超椭圆曲线有理点的有效计数方法；特点之三，用系统的数学方法讲述了椭圆和超椭圆曲线离散对数攻击的主要有效方法；特点之四，我们总是从算法数论的角度进行论述，对每个重要的理论结果，总是尽可能给出其可编程的实际算法. 本书的部分较初等的内容曾多次在中国科学院研究生院信息安全重点实验室及广州大学和湖南大学作为研究生教材使用.

本书可作为信息安全、数论及相关专业的研究人员、高等学校的教师和高年级学生的参考书，其部分内容也可做为信息安全、数论等专业的研究生的教材使用.

图书在版编目(CIP)数据

椭圆与超椭圆曲线公钥密码的理论与实现/王学理，裴定一 著. —北京：科学出版社，2006
(现代数学基础丛书；104)
ISBN 7-03-017358-9
I. 椭… II. ①王… ②裴… III. 椭圆曲线-密码-研究 IV. TN918.1
中国版本图书馆 CIP 数据核字(2006) 第 057318 号

责任编辑：陈玉琢 / 责任校对：包志虹
责任印制：安春生 / 封面设计：王 浩

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

新 蕾 印 刷 厂 印刷

科学出版社发行 各地新华书店经销
*
2006 年 12 月第 一 版 开本：B5(720×1000)
2006 年 12 月第一次印刷 印张：30 3/4
印数：1—3 000 字数：586 000

定价：65.00 元
(如有印装质量问题，我社负责调换〈环伟〉)

《现代数学基础丛书》序

对于数学研究与培养青年数学人才而言，书籍与期刊起着特殊重要的作用．许多成就卓越的数学家在青年时代都曾钻研或参考过一些优秀书籍，从中汲取营养，获得教益．

20 世纪 70 年代后期，我国的数学研究与数学书刊的出版由于文化大革命的浩劫已经破坏与中断了十余年，而在这期间国际上数学研究却在迅猛地发展着．1978 年以后，我国青年学子重新获得了学习、钻研与深造的机会．当时他们的参考书籍大多还是 50 年代甚至更早期的著述．据此，科学出版社陆续推出了多套数学丛书，其中《纯粹数学与应用数学专著》丛书与《现代数学基础丛书》更为突出，前者出版约 40 卷，后者则逾 80 卷．它们质量甚高，影响颇大，对我国数学研究、交流与人才培养发挥了显著效用．

《现代数学基础丛书》的宗旨是面向大学数学专业的高年级学生、研究生以及青年学者，针对一些重要的数学领域与研究方向，作较系统的介绍．既注意该领域的基础知识，又反映其新发展，力求深入浅出，简明扼要，注重创新．

近年来，数学在各门科学、高新技术、经济、管理等方面取得了更加广泛与深入的应用，还形成了一些交叉学科．我们希望这套丛书的内容由基础数学拓展到应用数学、计算数学以及数学交叉学科的各个领域．

这套丛书得到了许多数学家长期的大力支持，编辑人员也为其付出了艰辛的劳动．它获得了广大读者的喜爱．我们诚挚地希望大家更加关心与支持它的发展，使它越办越好，为我国数学研究与教育水平的进一步提高作出贡献．

杨　乐

2003 年 8 月

前　言

公钥密码是 20 世纪 70 年代中期提出的一类新型的密码, 它特别适合在计算机网络环境下使用, 具有信息加密、管理密钥和数字签名等功能, 能保证信息的机密性、完整性和不可否认性. 迄今为止, 所提出的公钥密码的安全性均建立于某个数学难题的基础之上, 这里所谓数学难题, 是指求解这个数学问题目前还没有多项式时间的算法被发现, 例如, 大整数的因子分解、有限域或椭圆曲线离散对数等问题, 在适当选取参数后, 在现有理论和技术条件下, 这些问题都难以解决, 这就奠定了相应的公钥密码的安全性基础, 而解决这些难题所取得的任何重大进展, 都会对相应的公钥密码的使用产生巨大的影响.

目前影响最大的三类公钥密码是 RSA 公钥密码、ElGamal 公钥密码和椭圆曲线公钥密码, 前者是在 20 世纪 70 年代中期提出的, 其安全性依赖于大整数的因子分解的困难性, 而后两者的安全性分别依赖于有限域和椭圆曲线离散对数的难度. 椭圆曲线公钥密码是 20 世纪 80 年代中期提出来的, 由于它具有一些其他公钥密码无法比拟的优势, 因此, 近年来对它的研究十分活跃, 而相关的研究所获得的许多算法, 大大丰富了算法数论和椭圆曲线密码的理论. 本书的主要目的就是介绍这方面的最新进展.

具有良好密码特性的椭圆曲线的产生和椭圆曲线离散对数的计算, 是椭圆曲线密码理论研究的两个核心问题, 而如何加快椭圆曲线的倍点运算, 则是椭圆曲线密码实现中的主要问题. 因此, 本书的主要内容就是介绍这三方面的基本理论, 及迄今为止所提出的主要算法的基本原理和实际算法实现. 主要内容分布如下: 本书分五大部分, 第一部分是椭圆曲线密码体制介绍, 我们的叙述方式利用了可证明安全性的理论框架; 第二部分是利用到整体域的提升方法计算有限域上椭圆曲线的有理点的数目, 主要包含复数域和一般域上椭圆曲线的一般理论以及复乘算法和 SEA 算法; 第三部分是利用到局部域的提升方法计算有限域上椭圆曲线的有理点的数目, 主要包含局部域上椭圆曲线的基本理论、形式群以及 Satoh 算法、AGM 算法、Harley 算法、Kedlaya 算法等内容; 第四部分介绍 (超) 椭圆曲线离散对数的攻击方法, 主要有基本的初等攻击方法、指标计算攻击方法、代数几何攻击和代数数论攻击方法; 第五部分介绍椭圆曲线的倍点计算, 这是椭圆曲线密码实现中的主要问题.

下面我们简单介绍一下上面提到的有关内容. 在第一章中, 我们介绍了 IEEE P1363 标准中推荐的有关加密、签名等方案, 从这些方案的介绍中可以看出, 若要

实现它们, 则要找到具有良好密码特性的椭圆曲线, 并考虑椭圆曲线离散对数的安全性, 同时加快椭圆曲线的倍点运算. 我们在介绍了这些方案后, 就利用所谓可证明安全性的框架对这些方案进行讨论. 需要指出的是, 现在人们一般认为, 应该要求所给方案在某种安全性框架 (或曰模型) 下是可证明安全的, 至于在实际应用中需要什么框架下的可证明安全性, 则需要根据实际情况来决定. 在第二部分中, 我们介绍提升到整体域的椭圆曲线有理点点数计算方法, 其理论基础是 Deuring 的相关理论, 简单地说, 就是一条定义在有限域上的通常的椭圆曲线都可以提升到某条定义在某个代数数域上的椭圆曲线, 而它在模去某个理想后, 就回到了原来的有限域上定义的椭圆曲线, 这个提升的过程就使我们能将有限域上的问题转化为复数域上的相关问题. 而在复数域上, 就有很多的可供利用的工具, 如复乘理论、模形式理论等, 这就分别构成了复乘算法和 SEA 算法的基础, 这些算法对大特征和小特征的有限域都可以应用. 在第三部分中, 我们将刚才的 Deuring 的理论中的整体域换成局部域 (相应的 Deuring 理论依然成立), 就将有限域上的问题转化为局部域上的相应问题, 而利用局部域和有限域上椭圆曲线的关系 (Lubin-Serre-Tate 定理), 就可以得出 Satoh 算法. 而利用椭圆曲线的 2- 同种方法到相关的局部域上的椭圆曲线, 我们就得出 Mestre 的 AGM 算法. 如果我们应用 de Rham 上同调等工具到定义在局部域上的相关几何对象上 (椭圆或超椭圆曲线), 就得到 Kedlaya 算法. 在第四部分中, 我们介绍目前已知的各种对 (超) 椭圆曲线密码的攻击方法, 除了一些较初等的方法外, 我们主要介绍的方法有两类, 即代数几何的方法和代数数论的方法, 这两类方法的思想都来自 Gerhard Frey, 前者的主要工具是 Weil 下降, 而后者的主要工具是类域论 (特别是 Brauer 群理论), 前者的想法是利用 Weil 下降将椭圆曲线离散对数问题转化为另一类几何对象 (例如, 超椭圆曲线或高维 Abel 簇) 的离散对数问题, 而后者的想法是利用类域论的方法将椭圆曲线离散对数问题转化为 Brauer 群中的对应问题. 我们认为这两类方法均具有很好的研究前景, 而且由于此前还没有任何著述系统介绍这两类方法, 所以我们希望有兴趣的读者能深入了解这些理论. 最后, 我们在第五部分介绍了如何加快倍点运算的各种方法.

本书的选材经过精心考虑, 内容的涉及面很广, 在有限的篇幅内包含了必要的预备知识和数学证明, 从而形成了一个完整的体系. 我们写作本书的一个主要思想是: 既系统介绍有关的理论, 又详细给出这些理论的相关算法, 这样就能够真正使理论和应用很好地结合. 我们希望, 读者无论是只对算法实现感兴趣 (如相关的工程技术人员), 或只对理论感兴趣 (如数学研究工作者), 或对两者均感兴趣 (如公钥密码研究者), 都能从中有所裨益. 本书可作为数论和信息安全专业的研究人员和研究生的参考书. 如果作为研究生的教材, 则需要根据学生的情况对有关内容进行取舍. 本书的部分内容曾在中国科学院研究生院信息安全国家重点实验室和广州大学及湖南大学作为研究生教材使用.

在本书的编写过程中, 作者王学理曾多次应 Gerhard Frey 教授邀请访问 Essen 大学 IEM, 在此表示衷心的感谢. 在本书写作过程中, 董军武同志给予了作者十分重要的帮助, 并写作了第十九章的内容, 而高伟同志写作了第一章的部分内容, 在此一并感谢. 另外, 本书的编写得到国家自然科学基金 "低权模形式的构造及其在二次型和椭圆曲线中的应用"(批准号：10271042) 和国家 "973" 项目 "信息与网络安全体系结构"(批准号：G1999035804) 的资助, 特此感谢.

最后, 作者王学理特别要感谢他亲爱的妻子徐东平女士和他可爱的两个女儿毛毛、虫虫以及他的双亲和岳父母, 是他们的支持和爱使本书的完成成为可能.

作　者

2005 年 4 月 21 日

目　录

第一部分　椭圆曲线密码体制

第二部分　提升到整体域上的点数计算算法

第三部分　提升到局部域上的点数计算算法

第四部分　椭圆曲线密码体制的攻击方法

第五部分　椭圆曲线密码体制的实现

*　　*　　*

第一部分

椭圆曲线密码体制

第一章　椭圆曲线密码体制

在本章中, 首先引进有限域上的椭圆曲线及其上的加法运算, 然后给出椭圆曲线公钥密码体制的加密、解密、签名等方案.

§1.1　有限域上的椭圆曲线

设 p 为一素数, n 为正整数, $q=p^n$, 而 $\mathbb{F}_q$ 是 q 个元素的有限域, 记 $\mathbb{F}_q$ 的代数闭包为 $\overline{\mathbb{F}}_q$. $\mathbb{F}_q$ 上的 Weierstrass 方程式

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,\quad a_i\in\mathbb{F}_q. \tag{1.1}$$

决定仿射平面 $\mathbb{A}^2(\overline{\mathbb{F}}_q)$ 上一条曲线, 添加上无穷远点后, 就得到射影平面 $\mathbb{P}^2(\overline{\mathbb{F}}_q)$ 上的一条曲线 E, 若曲线 E 是非奇异的, 则 E 称为一条椭圆曲线. 可以证明 E 是一条椭圆曲线, 当且仅当判别式 $\Delta\neq 0$, 其中

$$\begin{aligned}
\Delta &= -b_2^2b_8-8b_4^3-27b_8^2+9b_2b_4b_6,\\
b_2 &= a_1^2+4a_2,\\
b_4 &= 2a_4+a_1a_3,\\
b_6 &= a_3^2+4a_6,\\
b_8 &= a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2.
\end{aligned} \tag{1.2}$$

有关证明参见 §3.1. 我们定义 E 的 j 不变量如下:

$$j=c_4^3/\Delta,\quad c_4=b_2^2-24b_4. \tag{1.3}$$

给定一条 $\mathbb{F}_q$ 上的椭圆曲线 E, 及其上任意两点 P 和 Q, 连接 P 和 Q 的直线与 E 交于第 3 个点 R, 由 R 和无穷远点 $\mathcal{O}$ 可决定一直线, 该直线与 E 的第 3 个交点定义为 P 与 Q 的和, 记为 $P\oplus Q$. 可以证明这样定义 E 上点的加法后, 就使 E 成为一个 Abel 群. 由上面的加法的定义, 可给出具体的加法公式如下:

设 E 是由 (1.1) 式定义的椭圆曲线, 我们有

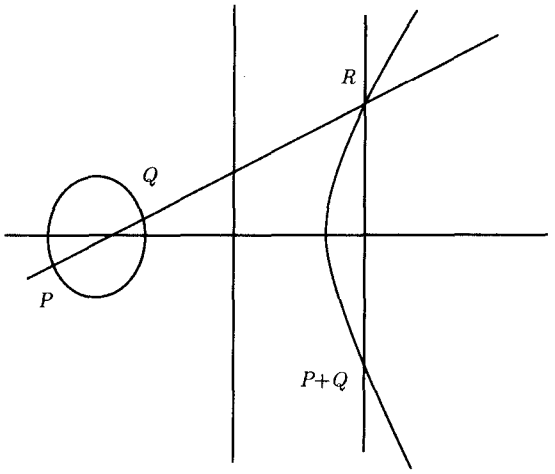
(a) 设 $P=(x,y)\in E$, 则 $-P=(x,-y-a_1x-a_3)$, 设

$$P_1+P_2=P_3,\quad P_i=(x_i,y_i)\in E,\quad i=1,2,3.$$

(b) 若 $x_1 = x_2$, $y_1 + y_2 + a_1x_1 + a_3 = 0$, 则 $P_1 + P_2 = \mathcal{O}$, 否则, 令

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{当 } x_1 \neq x_2 \text{ 时,} \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \text{当 } x_1 = x_2 \text{ 时,} \end{cases}$$

$$v = y_1 - \lambda x_1.$$



(c) P_3 由下式给出:

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3.$$

特别地, 当 $P_1 \neq P_2$ 时,

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_x - x_1 - x_2,$$

当 $P_1 = P_2$ 时,

$$x(2P_1) = \frac{x_1^4 - b_4x_1^2 - 2b_6x_1 + b_8}{4x_1^3 + b_2x_1^2 + b_4x_1 + b_6},$$

其中 b_i 如 (1.2) 式定义.

另外, 可以证明, 当 $p \neq 2, 3$ 时, 每一条 $\mathbb{F}_q$ 上的椭圆曲线都同构于下述形式的一条椭圆曲线:

$$E: \quad y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q.$$

当 $p=3$ 时, $\mathbb{F}_q$ 上每一条椭圆曲线均同构于

$$E: \quad y^2=x^3+a_4x+a_6, \quad 若\ j=0,$$

或

$$E: \quad y^2=x^3+a_2x^2+a_6, \quad 若\ j\neq 0.$$

当 $p=2$ 时, $\mathbb{F}_q$ 上每一条椭圆曲线均同构于

$$E: \quad y^2+a_3y=x^3+a_4x+a_6, \quad 若\ j=0,$$

或

$$E: \quad y^2+xy=x^3+a_2x^2+a_6, \quad 若\ j\neq 0.$$

现在令

$$E(\mathbb{F}_q)=\{(x,y)\in E|x\in\mathbb{F}_q, y\in\mathbb{F}_q\}\bigcup\{\mathcal{O}\}.$$

不难看出, $E(\mathbb{F}_q)$ 是 $E(\overline{\mathbb{F}}_q)$ 的一个子群. 可以证明

$$|\#E(\mathbb{F}_q)-q-1|\leqslant 2\sqrt{q}$$

(参见 §3.5).

一般来说, 我们总是选取有限域 $\mathbb{F}_q$ 为下述二者之一: 或者 $\mathbb{F}_q$ 是一个素域 $\mathbb{F}_p$, 或者 $\mathbb{F}_q$ 是 $\mathbb{F}_{2^m}$(m 为某个素数), 我们这样选取是为了安全性的考虑 (参见本书第四部分).

§1.2 椭圆曲线公钥密码体制

一、体制建立

首先建立椭圆曲线密码体制: 选取一个基域 $\mathbb{F}_q$, 它或者是一个素域 $\mathbb{F}_p$, 或者是一个特征 2 的域 $\mathbb{F}_{2^m}$, 其中 m 为素数. 然后选取 $\mathbb{F}_q$ 上的一条椭圆曲线 E, 使其阶为一个大素数 n, 或者是一个大素数 n 与另一个小整数的乘积. 而后, 选取 E 上的一个阶为该大素数 n 的点 P. 于是, 有限域 $\mathbb{F}_q$、曲线 E、点 P 和其阶 n 均为公开的信息.

二、密钥生成

每一个参与者 (或者说用户)A 完成下述过程:

1. 随机选取一个整数 $d_A\in[1,n-1]$;
2. 计算点 $Q_A=d_AP$;
3. 该参与者的公钥为点 Q_A;
4. 该参与者的私钥为整数 d_A.

三、椭圆曲线加密方案 (ECES)

现在设用户 B 要发送信息 M 给用户 A, 则 B 的加密过程如下：

1. 找出 A 的公钥 Q_A;

2. 将信息 M 表示为一个域元素 $m \in \mathbb{F}_q$;

3. 随机选取一个整数 $k \in [1, n-1]$;

4. 计算点 $(x_1, y_1) = kP$;

5. 计算点 $(x_2, y_2) = kQ_A$, 若 $x_2 = 0$, 则返回第 3 步;

6. 计算 $c = m \cdot x_2$;

7. 将已加密数据 (x_1, y_1, c) 发送给 A.

而 A 收到密文 (x_1, y_1, c) 后的解密过程如下：

1. 计算点 $(x_2, y_2) = d_A(x_1, y_1)$, 得出 $x_2 \in \mathbb{F}_q$;

2. 计算 $m = c \cdot x_2^{-1}$, 得出信息 M.

下面我们讨论该方案的安全性与问题难解性假设之间的关系. 我们不打算从严格形式化的角度来讨论密码系统的安全性, 而是更多地专注于密码学的数学理论. 如对严格定义和形式化证明感兴趣 (如概率多项式时间算法、不可忽略性、显著、CCA,CPA 等), 可参看文献 [1].

定义 1.1 (全有或全无安全性 (all-or-nothing))　在此模型下, 对给定的加密算法及一个给定密文, 攻击者的目的是计算与之对应的整个明文; 或者根据加密算法及给定的一个明密文对, 攻击者试图计算出该算法对应的整个解密密钥. 攻击者要么成功即能够获得整个明文分组或者解密密钥, 要么失败即没有获得任何信息. 这里所谓“没有任何信息”是指攻击者无论攻击前后都没有掌握所要攻击的目标 (整个明文或解密密钥) 的任何信息.

定义 1.2 (被动攻击)　在该模型下, 攻击者不能操纵和修改它所掌握的密文, 并且不能从加密方获得 (对非攻击目标的) 加密或解密服务.

定义 1.3 (选择明文攻击 (CPA))　在这种攻击模型下, 攻击者可以选择任何明文并且获得其相应的密文, 并在此基础上试图降低密码系统的安全性 (如对于攻击的目标密文, 获得明文的若干比特, 或者获得整个明文).

易知, 对于任何的公钥密码系统, 攻击者可以根据加密算法和加密公钥发起选择明文攻击.

定义 1.4 (椭圆曲线计算性 Diffie-Hellman 问题 (ECCDH))

Input：基域 $\mathbb{F}_q$ 及其上的椭圆曲线 E, E 上的阶为素数 n 的点 P, aP, bP, 这里 $a, b \in_R \mathbb{Z}_n^*$ (这里符号 $\in_R$ 表示随机均匀选取, 以下同).

Output：abP.