ELLIPTIC CURVE

椭圆曲线密码快速算法理论

丁勇 著

人民邮电出版社
POSTS & TELECOM PRESS

桂林电子科技大学学术著作出版基金资助出版

ELLIPTIC CURVE

椭圆曲线密码快速算法理论

丁勇 著

人民邮电出版社
北京

图书在版编目（CIP）数据

椭圆曲线密码快速算法理论 / 丁勇著. — 北京 : 人民邮电出版社, 2012.10
ISBN 978-7-115-28943-8

Ⅰ. ①椭… Ⅱ. ①丁… Ⅲ. ①椭圆曲线—算法理论 Ⅳ. ①O187.1

中国版本图书馆CIP数据核字(2012)第169133号

内 容 提 要

本书以作者及其研究组多年的研究成果为主体，结合国内外专家及学者在椭圆曲线密码快速算法方面的代表性成果，系统论述了这一领域的主要研究内容。本书分为两个部分，共7章。第一部分（第1、2章）讲述了研究椭圆曲线密码体制所需的基础知识及椭圆曲线上点的计算；第二部分（第3～7章）讲述了椭圆曲线密码的快速算法及其分析，主要包括非邻接形式（NAF）的改进形式，基于最大公约数（GCD）算法的高速带模除法，基于多基表示的快速算法，基于双基数链的Tate对优化算法。

本书既可以作为密码学、信息安全、计算机科学等相关专业的研究生教学参考书，也可作为教师和相关科研人员的参考书。

椭圆曲线密码快速算法理论

◆ 著　　丁　勇
责任编辑　王建军
执行编辑　代晓丽
◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷
◆ 开本：787×1092　1/16
印张：11　　2012年10月第1版
字数：245千字　　2012年10月河北第1次印刷
ISBN 978-7-115-28943-8
定价：45.00元
读者服务热线：(010)67119329　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

自从 W.Hellman 和 M.E.Hellman 于 1976 年提出公钥密码思想以来，由于其良好的性质以及现代通信网络的发展对信息安全技术需求的强烈增长，公钥密码体系得到了广泛的应用和发展。目前使用较为广泛的公钥密码体系是 RSA，但是它也有其局限性，由于存在着亚指数攻击，随着计算能力的不断增强，RSA 不得不提高密钥长度来保证其安全强度。1985 年提出的椭圆曲线密码体系（ECC，Elliptic Curve Crypto System）是一种基于椭圆曲线群上的新的公钥体系，相对 RSA 而言，它具有安全强度高、密钥长度短、计算速度快、节约通信带宽、节省存储空间等优点，逐渐成为理论研究的热点和实际应用的首选。而对于 ECC 的快速实现来说，最为关键的因素就是标量乘法 kP 的计算，因此研究标量乘法的快速算法具有很好的应用前景和迫切的实际需求。

1948 年 Shannon 发表了划时代的“通信的数学理论”[1]，宣告了信息论的诞生。60 多年后的今天，通信、计算机和网络技术的发展已将人类社会推进了一个崭新的信息时代。随着计算机及通信技术的快速发展，数字化、信息化、网络化正冲击、影响并改变着我们生活的方方面面。

自古以来，通信安全保密就成为各国军队和政府高度关注和把持的领域。孙子兵法云：“知己知彼，百战不殆”。因此，如何保证己方信息不被敌方知道就成了战场上的一个决定胜负的因素。历史上的战争，特别是在两次世界大战中，谁能在通信保密、密码分析上占据优势，往往就能在战争中取得主动，有些时候甚至成为扭转战局的关键。因此，早期密码的主要应用就是使用对称加密体制对通信的信息进行加密，以保证自己的情报不被敌方获悉。

在信息社会中，信息是一种重要的战略资源，因特网已经成为世界各国获取经济、军事和科技情报的极其重要的战场。信息高速公路为跨国搜集各种战略信息提供了新的机会，国际上围绕信息的获取、使用及控制的斗争亦愈演愈烈。“谁掌握了信息，控制了网络，谁就将拥有整个世界”（托夫勒）。一个国家的信息获取能力及在社会生产生活领域中“制信息权”的大小，成为了这个国家在生存与发展的竞争中能否占据主动的关键。信息安全已成为信息社会亟需解决的重要问题之一。在 21 世纪，保障信息安全是综合国力、经济竞争能力和生存能力的重要组成部分，是当前世界各国奋力攀登的制高点。

自从 20 世纪 70 年代中期 Diffie 和 Hellman 提出了公钥密码体系的思想[2]以来，密码学中爆发了一场革命。从那时起，密码学理论和技术已不再是被少数人掌握并服务于政府、军事、外交等神秘领域，而是“飞入寻常百姓家”。基于文献[2]思想的公钥密码体系以及 1977 年美国 NBS 制定的公开的数据加密标准 DES（Data Encrypt Standard）[3]成为了现代密码学诞生的两个标志。公钥体制的最大特点就是采用两个密钥将加密和解密功能分开：一个公开作为公钥（它的名称由此而来）；一个为用户专用，作为私钥。通信双方无

需事先交换密钥就可以进行保密通信，而要从用户公开的公钥以及可得的明文和密文中分析出私钥在计算上是不可行的。若以公钥作为加密密钥，以私钥作为解密密钥，可实现多个用户加密的消息只能由一个用户解读。反之，如果使用私钥作为加密密钥而将公钥作为解密密钥，则可实现一个用户加密，多个用户解读。公钥体制的出现，标志着保密学理论与技术划时代的革命的爆发，主要体现在以下几方面：第一，传统的对称加密体制主要功能是信息保密，而公钥体制则还可以实现消息的认证；第二，公钥体制无需实现交换密钥，大大简化了密钥分配的工作量，尤其适用于当前的大型动态网络；第三，公钥体制实现了密码学和数学（如数论、抽象代数、复杂性理论、组合数学、概率论等）、信息论、计算机科学以及微电子、量子理论等学科的交叉，大大丰富了密码学的内容，为密码学的研究提供了强有力的理论工具和应用领域。

基于 Diffie-Hellman 的思想，公钥密码算法的设计成为了密码学家研究的重点。许多密码学家提出了各种不同的公钥密码算法，有的是成功的，而有的是失败的。包括背包体制[4~7]、Willamas 体制[8, 9]、ELGamal 体制[10, 11]、RSA 体制[12~14]、椭圆曲线密码[15, 16]以及新兴的辫群公钥密码体系[17~20]和 NTRU[21]等。

由于公钥密码体系良好而特殊的性质，当前信息技术的高度发达导致的信息安全需求的多样性和爆发性，它被广泛地应用于信息安全的各个领域，用于构造各种密码应用和安全保护，如消息加密、认证和密钥协商、身份认证、数字签名、数据完整性保护、特殊数字签名、电子选举、电子商务等，特别是以 CA 和证书为支撑的 PKI 更是成为构建大型动态安全网络必需的基础设施。

在公开密码体制中，密钥对的选择要保证从公钥求出私钥等价于要求解一个困难的计算问题。公开密钥方案要求参与通信的双方知道一对密钥：私钥不能被其他参与方知道；公钥则以公开的方式保存起来，以便在同一安全方案下的参与方都知道。私钥和公钥通过单项函数联系起来：知道私钥可以很容易地得到公钥，但是知道公钥却很难得到私钥。通常情况下，公钥连同公钥算法一起保存在软件中，而私钥则以硬件的形式保存起来，避免对私钥的截取和篡改。对于 N 个通信方的网络来说，一方若需要跟网络中任何一方进行安全通信，则只需要保存自身的一个私钥，与其他参与方通信的时候查找相应的公钥即可。很明显，这种方案很好地解决了对称密钥方案的密钥管理问题，更主要的是，有些公开密钥算法可进行数字签名。构成常用公钥密码基础的困难问题是如下的数论问题。

1．整数的因子分解问题，其困难性是 RSA 公钥密码安全性的基础。

2．离散对数问题，其困难性是 EIGamal 公钥密码及其变体（如数字签名算法）安全性的基础。

3．椭圆曲线离散对数问题，其困难性是椭圆曲线公钥密码安全性的基础。

目前广泛应用于实际系统的公钥密码算法是 RSA 体制。它的困难性问题是基于大整数的因式分解问题，而大整数的因式分解问题是数学上的著名难题，至今没有有效的方法予以解决，因此可以确保 RSA 算法的安全性。该体制简述如下：独立地选取两个大素数 p、q，计算 $n=pq$，其欧拉函数 $\phi(n)=(p-1)(q-1)$；随机选择一个整数 $1\leqslant e<\phi(n)$，计算

$d=e^{-1}(\mathrm{mod}\ \phi(n))$，取公钥为 n、e，私钥为 d。对于明文 m，加密算法为 $c=m^x \bmod n$，其中 x 为 e（公钥加密）或者 d（私钥加密）。

椭圆曲线作为代数几何中的一个重要问题，已经有 100 多年的研究历史，积累了大量的研究文献。直到 1985 年，Kolitz 以及 Miller 才分别独立将其引入密码学领域，构造了 ECC（椭圆曲线密码体系）。相对 RSA 而言，椭圆曲线密码的优势和好处为：第一，安全强度更高。RSA 中存在着一般数域筛（NFS）方法攻击，使得其安全强度为亚指数级，而 ECC 的安全强度为指数级[22]，即使使用目前国际上公认的有效攻击方法——Pollard orhd 方法也很难将其破解。第二，密钥短。在同等安全强度下，椭圆曲线密码的密钥尺寸比 RSA 体制和 ElGamal 类体制要小得多，椭圆曲线密码所具有的短密钥这一优势，将适合在存储受限的条件下（如 IC 卡技术等）使用。第三，椭圆曲线密码所需的存储空间小，宽带要求低。由于其存储少、宽带要求低的特点，使得椭圆曲线密码在许多条件受限的领域内具有很优越的发展前景。第四，椭圆曲线密码的计算速度快。在现代分布式网络中，由于服务器的瓶颈效应，使得快速的认证成为了一种迫切的需求。比如一个 Web 服务器，如果认证速度太慢，就会影响用户访问的热情，导致服务效率降低。由于 ECC 最底层的有限域规模较小，以及相关研究的不断深入，已使得其计算速度大大高于 RSA 的计算速度。而相对后来的辫群公钥系统以及 NTRU 的新兴公钥系统，ECC 已经得到了广泛而长期的研究和攻击，能提供更可靠的安全性。

推动 ECC 实际应用的一个里程碑事件就是椭圆曲线数字签名标准（ECDSA）[23]（ANSI X9.62）的公布。之后其他国际组织也纷纷将其标准化，例如 IEEE P1363、ISO、IEC CD14888-3 等[24]，而相应的各种协议也将 ECC 应用到其中，如 IPSec/IKE[25, 26]、WAPI[27] 等。其中，由 Visa 和 Mastercard 两大信用卡公司于 1997 年推出的 SET（安全电子交易）协议更是将其默认的公钥密码算法置为 ECC。ECC 的加密技术产品已经被广泛应用到各种安全产品中，如 VPN 网关、防火墙，安全网关、安全路由器、Web 服务器、基于 ECC 的移动终端、SIM 卡数字签名模块、无线 POS 机、CA 以及基于 ECC 的企业级安全解决方案等。可以说 ECC 已经逐步并将最终取代 RSA 的主流应用公钥密码算法的地位，将拥有非常广阔的市场。

尽管现有的 ECC 的计算速度已经比 RSA 快了很多，但是由于信息技术飞速发展造成的信息膨胀，因此对 ECC 的计算速度也提出了更高的要求。ECC 的快速实现算法将在很长一段时间内成为安全专家研究的重点。

在对椭圆曲线密码的研究中，椭圆曲线密码的构造、分析和快速实现是目前研究的 3 个主要方向。由于椭圆曲线密码快速实现直接影响了整个椭圆曲线密码体系的性能，所以快速计算的实现已成为椭圆曲线密码体制能否快速实现的关键，本书主要对椭圆曲线密码快速算法进行了较深入的研究。

经过 10 多年来的努力研究，密码学家们在 ECC 标量乘法的快速计算方面取得了令人瞩目的成就。Knuth 提出了标量 k 从右到左的二进制方法。1997 年，J.Solinas 在二进制方法的基础上，提出了 k 的非邻接形式（NAF）和窗口 NAF 方法，此后不久又有学者在此

基础上提出了滑动窗口方法，这种方法利用额外的存储器，扩大了可能的系数集，降低了标量 k 的非零密度。目前基于 NAF 的研究有很多，其中主要的研究是与底层域上的快速算法相结合提出新算法。

目前研究最热的是由 V.S.Dimitrov 等人率先提出的双基数字系统（DBNS，Double-base Number System），此系统的思想是将标量 k 分解成 2 与 3 的幂指数和的形式，减少点加操作的次数。在双基数字系统的基础上，C. Doche 和 L. Imbert 提出了 Extended DBNS 方法，这种方法扩大了可能的系数集，有效地降低了椭圆曲线密码系统的计算复杂度。K.W.Wong 等人在双基表示的基础上，结合半点运算提出了一种新的双基表示，进一步提高了标量乘法的运算效率。近年来，Dimitrov 等人对双基数字系统进行了扩展，提出了多基的思想，基于多基思想的研究也是最近几年的研究热点。不少专著和文献对标量 k 的表示形式进行了更加深入的研究，在标量 k 的表示方面技术已愈趋成熟。基于双基系统的快速算法的相关研究可参考文献[28～30]。

近年来底层运算有了新的发展，Guajardo 等人应用中间变量，用乘法运算来代换求逆运算，提出了二进制域上 $4P$、$8P$、$16P$ 的直接计算方法，减少了算法的运算量。目前底层运算已经发展到了 $3P$、2^kP 等。

二进制域上的特殊曲线——Koblitz 曲线上的标量乘法由于可以不用使用倍点算法，而且其计算相对比较容易，所以，Koblitz 曲线的研究也是目前标量乘法研究的主要内容。

另外，Sakai 等人于 2000 年提出了基于双线性对的身份认证协议，最近几年，双线性对获得了广泛的密码应用，涌现出了各种基于双线性对的密码协议。实现这些应用的效率，取决于双线性对的计算速度，而实现这些协议的瓶颈在于能否快速计算双线性对，Miller 算法成功地运用倍点—加和切—割线组合来完成这一计算过程。

在 ECC 的标量乘法的快速计算方面的理论已愈趋成熟，而在 ECC 的快速实现中，最关键的因素就是标量乘法 kP 的快速算法研究问题。因此，研究这个问题有着较深的理论意义，更具有迫切的实际意义和广阔的市场前景。

本书的内容安排如下。第 1 章介绍椭圆曲线密码的基本概念和研究椭圆曲线密码所需的基础知识。第 2 章介绍椭圆曲线上重要的点的计算公式。第 3 章讲述了基于 NAF 分解，提出几种新的标量乘快速算法，如 w-NNAF 方法、RTSNAF 方法等。这些方法使得标量乘的计算复杂性可以进一步降低，最后定量分析了这些方法降低的计算复杂度。第 3 章是本书的重点。第 4 章讲述了联合稀疏形（JSF）与 Frobenius 映射结合的快速算法，该方法以少量的存储为代价获得了一定的运算加速。第 5 章介绍基于最大公约数（GCD）的高速带模除法，主要对常规 GCD 算法进行了深入分析，改进了算法的判断标准和体系结构，从根本上加快了 GCD 算法的效率。第 6 章扩展了基于半点与双基表示的 ECC 快速标量算法，分析并比较了提出的快速算法的计算复杂度相比于其他算法的优势。第 7 章提出了一种优化算法，将双基数链与 Miller 算法相结合，从而缩短了链长，减少了算法中的迭代次数，并将“倍点—加”的过程进行优化，提出新的除子表达式，在迭代过程中优化了除子计算，提高了运算速度。

目　录

第 1 章　椭圆曲线密码简介

椭圆曲线是代数几何中一类重要的曲线，至今已有 100 多年的研究历史。而应用于密码学中的椭圆曲线是基于有限域上的，通过引入无穷远点，将椭圆曲线上的所有点和无穷远点组成一个集合，并在该集合上定义一个运算，从而该集合和运算构成了群。在有限域上的椭圆曲线群有两种，分别基于 GF(p)以及 GF(2^m)，它们各自有不同的群元素和群运算，然而对于群上的 ECDLP 问题，都认为是一个指数级的困难问题。基于这个困难问题，构建了 ECC 算法，包括公钥加密、私钥解密、数字签名、签名验证、DH 交换等。

1.1　无穷远点

在平面上，任意两条不同的直线只有相交和平行两种关系，为了将这两种关系统一，引入了无穷远点的概念，无穷远点就是两条平行直线的交点。有了这个概念，我们就认为平面任意两条不同的直线都是相交的，对于平行的直线，它们的交点为无穷远点。任何一条直线有且只有一个无穷远点，平面上不平行的两条直线有不同的无穷远点。平面上所有的无穷远点组成一条直线，成为无穷远直线。

为了从坐标上把普通点和无穷远点表示出来，我们使用齐次坐标（X，Y，Z）（X，Y，Z 不能全为 0）来表示平面上普通坐标为（x，y）的点。二者之间的转化关系为 $x=X/Z$，$y=Y/Z$，之所以称为齐次坐标，是因为（pX，pY，pZ）表示同一个点。而无穷远点的齐次坐标表示形式为（X，Y，0），无穷远直线的方程为 $Z=0$。假设在普通的坐标系下一条直线 L 的方程为：$ax+by=c$，则在齐次坐标下 L 的方程为 $aX+bY=cZ$。任何曲线都可以实现方程之间的转化，而且任何曲线都包括无穷远点。

1.2 数论相关概念

1.2.1 同余和剩余类的概念

这一节我们将给出同余系统的一些结果。

定理 1.2.1 对整数 $n>1$，同余关系（模 n）具有自反性、对称性和传递性，即对任意的 $a, b, c \in Z$ 有

1．$a \equiv a \pmod{n}$；

2．如果 $a \equiv b \pmod{n}$，则 $b \equiv a \pmod{n}$；

3．如果 $a \equiv b \pmod{n}$，$b \equiv c \pmod{n}$，则 $a \equiv c \pmod{n}$。

满足定理 1.2.1 中 3 条性质的关系被称为等价关系。

大家都知道，一个集合上的等价关系把这个集合分为若干个等价类。令“$\equiv_n$”表示模 n 同余的等价关系。这个关系定义在集合 Z 上，因此它把 Z 恰好分成 n 个等价类，每个类包含于某整数模 n 同余的所有整数。把这 n 个类表示成

$$\bar{0}, \bar{1}, \cdots, \overline{n-1}$$

其中，$\bar{a} = \{x \in Z \mid x \pmod{n} \equiv a\}$。

我们将上面每一个集合均称为一个模 n 剩余类，显然，我们可以将 Z 看做是 $Z_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$。

定理 1.2.2 对任意的 $a, b \in Z$ 定义剩余类 $\bar{a}$ 和 $\bar{b}$ 之间的加法和乘法运算为

$$\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a} \cdot \bar{b} = \overline{ab}$$

则对任意的 $n>1$，由“$\pmod{n}$”定义的映射 $f: Z \to Z_n$ 是从 Z 到 Z_n 的一个同态映射。

定理 1.2.3 对任意整数 $n>1$，如果 $a \equiv b \pmod{n}$ 和 $c \equiv d \pmod{n}$，则 $a \pm c \equiv b \pm d \pmod{n}$，$ac \equiv bd \pmod{n}$。

1.2.2 Euler 定理和中国剩余定理

定义 1.2.1 Euler 函数。

在有限域 F_q 上，$q \geq 1$，在 $\{1, 2, \cdots, n\}$ 中与 n 互素的元素的个数叫做 Euler 函数，记作 $\phi(n)$。

引理 1.2.1 设 $\phi(n)$ 是定义 1.2.1 中定义了的欧拉 ϕ 函数。则

1．$\phi(1)=1$；

2．如果 p 是素数，则 $\phi(p)=p-1$；

3．欧拉 ϕ 函数是积性函数。即如果 $\gcd(m,n)=1$，则 $\phi(m,n)=\phi(m)\,\phi(n)$。

4．如果 $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ 是 n 的素分解，则

$$\phi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)。$$

定理 1.2.4　对于整数 $n\geqslant 0$，有 $\sum_{d|n}\phi(d)=n$。

证明　假设 $S_d=\{x\,|\,1\leqslant x\leqslant n,\gcd(x,n)=d\}$，显然，对于每个 $d\,|\,n$，集合 $S=\{1,2,\cdots,n\}$ 被分割成不相交的子集 S_d，所以

$$\bigcup_{d|n}S_d=S$$

注意到对任意的 $d\,|\,n$，有 $\#S_d=\phi(d/n)$，于是

$$\sum_{d|n}\phi(d/n)=n$$

然而，对任意的 $d\,|\,n$，我们有 $\phi(d/n)\,|\,n$，所以

$$\sum_{d|n}\phi(n/d)=\sum_{(d|n)|n}\phi(d/n)=\sum_{d|n}\phi(d)$$

证毕。

例 1.1　对于 $n=12$，$d\,|12$ 可能的值是 1，2，3，4，6 和 12。我们有

$$\phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(12)=1+1+2+2+2+4=12。$$

定理 1.2.5　Fermat 定理。

若 p 是素数，a 是正整数且不能被 p 整除，则

$$a^{p-1}\equiv 1 \bmod p$$

Fermat 定理的另一种有用的表示形式是若 p 是素数且 a 是正整数，则

$$a^{p}\equiv p \bmod p。$$

定理 1.2.6　Euler 定理。

令 $F_q^*=\{a\,|\,a\in F_q,\gcd(a,q)=1\}$，则 $F_q^*(q\geqslant 2)$ 中元素 a 满足

$$a^{\phi(q)}\equiv 1 \bmod q$$

其中，F_q^* 表示有限域中所有的非零元素的集合。

定理 1.2.7　中国剩余定理（CRT)。

令 r 个整数 $m_1,m_2,\cdots,m_r$ 两两互素，$a_1,a_2,\cdots,a_r$ 是任意 r 个整数，则同余方程

$$x\equiv a_i \bmod m_i,\quad 1\leqslant i\leqslant r \tag{1-1}$$

有如下唯一解

$$x=\sum_{i=1}^{r}a_iM_iy_i$$

其中，$M_i = M/m_i$，$M = m_1 m_2 \cdots m_r$，$y_i = M_i^{-1} \bmod m_i$，$1 \leqslant i \leqslant r$。

算法 1.1 中国剩余算法

输入：整数多元组$(m_1, m_2, \cdots, m_r)$两两互素；

整数多元组$(a_1 (\bmod m_1), a_2 (\bmod m_2), \cdots, a_r (\bmod m_r))$

输出：整数$x < M = m_1, m_2, \cdots, m_r$满足方程（1-1）

1．$M \leftarrow m_1 m_2 \cdots m_r$

2．对于$i = 1, 2, \cdots, r$重复执行

（1）$y_i \leftarrow (M/m_i)^{-1} (\bmod m_i)$

（2）$\bar{1}_{m_i} \leftarrow y_i M/m_i$

3．返回$\left(\sum_{i=1}^{r} \bar{1}_{m_i} a_i (\bmod M) \right)$

中国剩余定理是数论中最有用的定理之一，它说明了某一范围内的整数可通过它对两两互素的整数取模所得的余数来重构。

1.3 有限域简介

有限域的具体相关知识请参看文献[31]。我们这里仅列出一些重要的概念和定理。

定义 1.3.1 任意给定一非空集合 G 和其上的二元运算“$*$”，如果满足：

1．封闭性：对任意$a, b \in G$，存在$c \in G$，使得$a * b = c$；

2．结合律：对于任意$a, b, c \in G$，都有$(a * b) * c = a * (b * c)$；

3．单位元 e 存在：即存在$e \in G$，对于任意$a \in G$，都有$e * a = a * e$；

4．逆元存在：对于任意$a \in G$，存在$b \in G$，使得$b * a = a * b = e$，b 称为 a 的逆元。

则称集合 G 关于二元运算“$*$”构成群，记为：<G，$*$>。

在群<G，$*$>中，如果对于任意$a, b \in G$，都有$b * a = a * b$，则称群<G，$*$>是交换群，也称为阿贝尔（Abel）群。

定义 1.3.2 设“+”，“$*$”是 G 上的二元运算，集合的基数$|G| > 1$，如果满足：

1．<G，+>是一个交换群，其单位元记为 0；

2．<$G - \{0\}$，$*$>是交换群，其单位元记为 1；

3．运算“$*$”对“+”可分配，即对任意$a, b, c \in G$，都有

$$a * (b + c) = (a * b) + (a * c)$$

$$(a + b) * c = (a * c) + (b * c)$$

则称<G，+，$*$>是域。

例如：<N，+>是自然数集上关于“+”所做成的群，<$Q*$，×>是非零有理数集关于

“×”所做成的群，而<Q，+，×>则是有理数集上关于“+”和“×”所做成的域。

定义 1.3.3　有限域，又称伽罗华（Galois)域，顾名思义，就是指域 G 元素个数为有限的域。其中，G 中的元素个数称为有限域 G 的阶，记为$|G|$。

定义 1.3.4　设 G 是任意域，1 是 G 的单位元。

如果对于任何正整数 n，有

$$\underbrace{1+1+\cdots+1}_{n\text{个}1}\neq 0$$

则称域 G 的特征为 0；

如果存在正整数 n，满足

$$\underbrace{1+1+\cdots+1}_{n\text{个}1}=0$$

则称满足上式的最小正整数 n 为 G 的特征，记为 $ChG=n$。

定理 1.3.1　若 G 是域，则 G 的特征为 0 或者是一个素数 p。

定理 1.3.2　从同构意义上来说，则只存在两种有限域。一种有限域元素个数为 p（p 为正素数），记做 GF(p)；另一种元素个数为 p^m（p 为正素数，m 为正整数），记做 GF(p^m)。

定义 1.3.5　有限域的全体非零元素都可以用域中某一个元素的幂次来表示，我们称这个元素为域的本原元。

定义 1.3.6　对于有限域上的一个元素 x，满足 $x^l=1$ 的最小的正整数 l 称作元素 x 的阶。

有限域 GF(p)可以用区间[0，p−1]上的全体整数来表示，并且满足如下条件。

1．乘法中的幺元为整数 1。

2．加法中的零元为整数 0。

3．域中的加法为模 p 加法，即任取 $a,b\in \mathrm{GF}(p)$，有 $a\oplus b=(a+b) \bmod p$。

4．域中的乘法为模 p 乘法，即任取 $a,b\in \mathrm{GF}(p)$，有 $a\otimes b=(a\times b) \bmod p$。

对于有限域 GF(p^m)，由于主流的 ECC 算法中只用到 GF(2^m)，因此我们这里只介绍 GF(2^m)，GF(p^m)的表示方式也和 GF(2^m)类似。GF(2^m)可以看做是 GF(2)上的一个 m 维向量空间，只要确定了空间上的基，GF(2^m)上的任何一个元素都可以用这些基的线性组合来表示。若用多项式基表示，首先确定一个 GF(2)上的 m 次不可约多项式 $f(x)$，则多项式 $x^i(0\leqslant i<m-1)$就构成了 GF(2^m)上的基，即 GF(2^m)上的任何一个元素都可以用它们的线性组合多项式 $\sum_{i=0}^{m-1}a_i x^i$（$a_i\in \mathrm{GF}(2)$）来表示。为了方便，我们用比特串 $(a_{m-1},a_{m-2},\cdots,a_1,a_0)$ 来表示。

因此，GF(2^m)对应所有次数小于 m 的 GF(2)上多项式，也对应于长度为 m 的所有比特串，并且有如下法则。

1．乘法幺元为 1，用 $(0,0,\cdots,0,1)$ 表示。

2．加法的零元为 0，用 $(0, 0, \cdots, 0, 0)$ 表示。

3．域上的加法为两个元素对应比特串的异或（XOR）运算。

4．令 a 的多项式表示为 $a(x)$，b 的多项式表示为 $b(x)$，$r(x)=a(x)b(x) \bmod f(x)$，则 $ab=r$。

对于有限域 GF(2^m)，总存在元素 $\beta \in \mathrm{GF}(2^m)$，使得 $\{\beta^{2^0}, \beta^{2^1}, \cdots, \beta^{2^{m-1}}\}$ 为 GF(2^m)的一组基，我们把这种形式的基称为正规基。任取一个元素 α，都可以唯一地表示为 $\alpha=\sum_{i=0}^{m-1} a_i \beta^{2^i}$（$a_i \in \mathrm{GF}(2)$），因此可用 m 长度的比特串 $(a_{m-1}, a_{m-2}, \cdots, a_1, a_0)$ 来表示。在正规基表示下，有如下的运算法则。

1．加法的零元为全 0 比特串。

2．乘法的单位元为全 1 比特串。

3．两个元素的加法为异或（XOR）运算。

4．乘法的运算可看做是关于 β 的两个多项式的乘积，再将其转化为标准形式。

使用正规基的一个最大的好处就是使得乘方运算非常简单，只需要一个右循环移位，尽管这样会使得不同的两个元素的乘积运算比较复杂，但是幸运的是对于不能被 8 整除的 m，总存在一种特殊的高斯正规基（GNB），在这种正规基下，乘法同样也能快速地计算。

1.4 椭圆曲线简介

1.4.1 椭圆曲线的概念

这里所说的椭圆曲线并不是通常意义的椭圆，它是一类特殊的曲线，有限域 K 上椭圆曲线的方程形式为

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1-2}$$

其中，$a_1, a_2, a_3, a_4, a_6 \in K$ 且满足 E 的判别式 $\Delta \neq 0$，则具体定义为

$$\begin{aligned} \Delta &= d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6, \\ d_2 &= a_1^2 + 2a_2, \\ d_4 &= 2a_4 + a_1a_3, \\ d_6 &= a_3^2 + 4a_6, \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2。 \end{aligned} \tag{1-3}$$

如果 L 为有限域 K 的扩域，则 $E(L)=\{(x, y) \in L \times L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{O\}$，这里符号 O 表示无穷远点。

上式即为著名的 Weierstrass 方程，由于 $a_1, a_2, a_3, a_4, a_6 \in K$，所以称 E 为 K 上的椭圆曲线，一般记为 E/F。需要注意的是，如果 E 定义在 K 上，则 E 必然定义在 K 的扩域上。

条件 $\Delta \neq 0$ 确保了椭圆曲线的光滑性，也就是说曲线上没有一个点有两个或者更多的