文章编号:1671-4229(2021)04-0016-13

离散对数求解算法

庄金成[1], 朱玉清[2]

(1. 山东大学 网络空间安全学院/密码技术与信息安全教育部重点实验室, 山东 青岛 266237;
2. 北京交通大学 智能交通数据安全与隐私保护技术北京市重点实验室/计算机与信息技术学院, 北京 100044)

摘 要: 离散对数问题是算法数论中的一个重要研究课题,而且有广泛的应用。特别地,离散对数问题的求解困难性是相关密码学方案安全性的基础。文章描述了以有限阶循环群为基本研究对象的离散对数问题定义和其变形,综述了离散对数问题的求解算法。首先,介绍了通用算法,其中量子算法可以高效求解一大类离散对数问题,而经典的通用算法时间复杂度较高。其次,展示了指标计算框架,在具体加速求解离散对数中有广泛的应用。最后,重点介绍基于有限域乘法单位群和椭圆曲线加法群离散对数的求解算法和相关进展。基于有限域乘法群单位群离散对数问题的求解困难性和有限域的特征密切相关,基于小特征的有限域离散对数可以设计更高效的求解算法。而目前求解一般椭圆曲线离散对数问题的经典算法仍然是指数时间的算法。

关键词: 离散对数问题; 算法; 有限域; 椭圆曲线

中图分类号: TP 309.7 **文献标志码**: A

Algorithms solving discrete logarithms

ZHUANG Jin-cheng[1], *ZHU Yu-qing*[2]

(1. School of Cyber Science and Technology/Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Qingdao 266237, China; 2. Beijing Key Laboratory of Security and Privacy in Intelligent Transportation/School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China)

Abstract: The discrete logarithm problem (DLP) is a research topic of great essence in algorithmic number theory, which also has diverse applications. In particular, the hardness of discrete logarithms underpins the securities of related cryptographic schemes. This article describes the basic version of DLP over a cyclic group of finite order and its variants, and surveys algorithms for discrete logarithms. First, generic algorithms are introduced, among which quantum algorithms can efficiently solve a certain class of DLP but classic algorithms occupy high time complexity. Then, the framework of index calculus method is presented, which has applications in accelerating algorithms for DLP in some specific scenario. At last, algorithms and progress for DLP over finite fields and elliptic curves are reported. DLP over finite fields is highly related with the characteristic of the finite field. Faster algorithms are designed for DLP over finite fields with small characteristics. In contrast, the state-of-the-art algorithms for general elliptic curve DLP run in exponential time.

Key words: discrete logarithm problem; algorithms; finite fields; elliptic curves

---

基金项目: 国家自然科学基金资助项目(62002015);国家重点研发计划资助项目(2018YFA0704702,2021YFB3100200);中央高校基本科研业务费专项资金资助项目(2021RC259);山东省自然科学基金重大基础研究资助项目(ZR202010220025)

作者简介: 庄金成(1987—),男,教授,博士. E-mail:jzhuang@sdu.edu.cn

引文格式: 庄金成, 朱玉清. 离散对数求解算法[J]. 广州大学学报(自然科学版),2021,20(4):16-28.

1　离散对数问题定义和应用

1.1　离散对数问题和应用

一般地,给定一个代数系统 G(运算记作乘法),元素 g 和幂数 x,指数运算是计算 g^x。指数运算的逆运算是对数运算,即给定元素 $g,h\in G$,求 x 使得 $g^x=h$,或者证明这样的 x 不存在。

特别地,当幂数属于一个离散集合(常用的是整数集合)时,对应的运算称为离散指数运算,对应的逆问题称为离散对数问题。本文主要讨论基于有限群的离散对数问题,基本的情形定义如下:给定一个有限群 $G,|G|=N$ 以及元素 $g,h\in G$,求解整数 $0\leqslant x\leqslant N-1$ 使得 $g^x=h$,整数 x 称为 h 相对于 g 的离散对数,也记为 $\log_g h$。

离散对数问题本身是算法数论中的一个重要研究问题。Gauss 证明模任意素数 p 存在原根,对应的指标求解问题就是一类重要的离散对数问题,在求解高次同余方程中有重要应用。和通常的对数一样,通过预先计算的离散对数可以将对应的乘法运算转化为加法运算。在通常离散对数定义变形得到的 Zech 对数(也称 Jacobi 对数)也有很多应用[1]。

离散对数问题在密码学中可以应用于线性反馈移位寄存器的生成序列和相关的伪随机数生成器[2]。1976 年,Diffie 等[3]提出了公钥密码学的概念,设想基于陷门单项函数设计公钥密码体制,并且在 Gill 的建议下采用模指数运算(其逆函数即为离散对数)为设想的单向陷门函数,在此基础上设计了第一个公钥密码系统,即 Diffie-Hellman 密钥交换体制。1978 年,Rivest 等[4]基于整数分解问题设计了第一个公钥加密和数字签名体制。离散对数和整数分解问题是经典的公钥密码体制中使用最广的 2 类困难问题,并且 2 者的求解算法有很多相似之处。

Diffie-Hellman 密钥交换体制优势之一是提供了前向安全性[5],此后离散对数问题被用来设计功能更丰富的密码体制。例如,ElGamal[6]基于离散对数问题设计了公钥加密方案,Schnorr[7]基于离散对数问题设计了身份认证和签名方案,美国国家技术标准局[8]基于离散对数制定了数字签名标准。此外,Diffie-Hellman 体制和 ElGamal 体制的设计思路还对后量子密码方案的设计有所启发,如基于编码的密码方案[9]、基于格上困难问题的 LPR 加密方案[10]。

公钥密码学中最早使用的离散对数问题是基于有限域的乘法群,后来扩展到基于其他代数的结构,包括基于椭圆曲线上有理点的加法群、基于超椭圆曲线的 Jacobian、基于代数数域的理想类群和基于特定代数整数环等[11]。其中,基于椭圆曲线的离散对数问题应用尤其广泛,具体定义是给定有限域 $\mathbb{F}_q$ 上的椭圆曲线 E 和有理点 $P,Q\in\langle P\rangle$,求解整数 x 使得 $Q=xP$。Miller[12]和 Koblitz[13]独立地提出基于椭圆曲线离散对数问题的密码学方案设计。椭圆曲线离散对数问题还应用在 SM2、SM9 和一些基于区块链技术的协议等密码方案中。

1.2　离散对数问题变体

根据不同的应用场景,上述基本的离散对数问题有一些变体。

在一些应用中可能限定离散对数的取值范围,或者通过侧信道等技术获得部分信息从而缩小了求解范围。例如,如果已知离散对数 $0\leqslant x<T$,对应的称为区间离散对数问题。

如果已知离散对数 x 的二进制中 1 的个数较少,对应的称为低 Hamming 重量离散对数问题。

如果给定一个生成元 g 和多个目标元素 $h_1,h_2,\cdots,h_n$,对应的称为多目标离散对数问题。

如果给定多个生成元素 $g_1,g_2,\cdots,g_n$ 和一个目标元素 h,对应的称为高维离散对数问题,也称为表示问题[14],可以应用于设计电子货币等。

实例压缩问题是指给定 m 个实例 $(g^{x_1},g^{x_2},\cdots,g^{x_m})$,是否可以压缩到 $n(n<m)$ 个实例 $(g^{y_1},g^{y_2},\cdots,g^{y_n})$,使得通过解决 $(g^{y_1},g^{y_2},\cdots,g^{y_n})$ 的离散对数可以高效恢复出 $(g^{x_1},g^{x_2},\cdots,g^{x_m})$ 的离散对数。

离散对数问题还有一种变体称为带辅助输入的离散对数问题,即在具有辅助输入 $g^x,g^{x^2},\cdots,g^{x^d}$ 的情形下加速离散对数 x 的计算。

1.3　离散对数问题扩展

Diffie 和 Hellman 设计的两方密钥交换协议基于的更精确的困难问题是 Diffie-Hellman 问题,随机选择整数 a,b,c,计算版本的定义是给定 g,g^a,g^b,计算 g^{ab}。判定版本是区分 g^a,b^b,b^{ab} 与 g^a,b^b,

g^c。基于 Diffie-Hellman 问题可以实现密钥交换协议,如基于身份的加密[15]、陷门函数[16]等。

离散对数问题和 Diffie-Hellman 问题之间是否等价是一个重要的公开问题。

Diffie-Hellman 问题的一个重要推广是基于双线性对的双线性 Diffie-Hellman 问题[17]。给定素数阶循环群 G_1, G_2, G_3,密码学中的双线性对是指存在如下映射

$$e: G_1 \times G_2 \to G_3,$$

满足双线性、非退化和易于计算的性质。密码学中常用的双线性对实例包括有限域椭圆曲线上的 Weil 对和 Tate 对。双线性对密码学包含了丰富的密码功能,包括3方的一轮密钥交互[18],基于身份的加密[19]、短签名[20]和群签名[21]等。

Boneh 等[22]设想了基于多线性映射可以设计功能更加丰富和强大的密码体制。

2 通用求解算法

2.1 随机自归约和比特困难性

在密码学应用中更多是按照一定的分布随机选择平均情况的实例,平均情形的困难性和最坏情形困难性的关系对于密码应用具有重要意义。

离散对数问题通过随机化方法可以建立最坏情况到一般情况的自归约[23]。假定要求的目标元素是 $h \in G = \langle g \rangle$,可以选取随机数 $r \bmod N$,计算平均情形的实例 $h' = hg^r$,如果可以求解 $\log h'$,就可以对应求解出 $\log h$。

一些格上的困难问题也可以建立最坏情况到一般情况的归约,如最小整数解问题(Short Integer Solution, SIS)和容错学习问题(Learning With Errors, LWE)。区别是离散对数是同一个群上的归约,而后者是从任意的格归约到给定的平均情形困难问题。

考虑一般循环群上的离散对数问题,如果 $G = \langle g \rangle$ 上的离散对数是困难的,Hastad 等[24]证明对于随机选取的满足 $|G| = q = p'2^k$,q 的二进制表示为 n 比特,那么 x 的 k 到 $n-1$ 比特以很高的概率是求解困难的。

2.2 量子算法

整数分解问题和离散对数问题既是公钥密码学应用最广泛的2类困难问题,针对2者的求解算法也有相似之处,包括量子算法和经典算法。Shor[25]设计了量子算法求解整数分解问题和素域上的离散对数问题。

2者都可以看作特殊的隐藏子群问题,例如,基于有限循环群上的离散对数计算等价于求解下面映射的核:

$$\varphi: \mathbb{Z}^2 \to G,$$

其中,$\varphi(a,b) = g^a h^b$。

更一般地,求解基于交换群的隐藏子群问题有高效的量子算法[26]。

下面讨论经典计算模型(如 Turing 机)下求解离散对数问题的算法。

2.3 Pohlig-Hellman 方法

Pohlig 等[27]提出了一种约化方法,假设已知群阶的素分解 $N = \prod_{i=1}^{n} p_i^{e_i}$,目标是求解 $x = \log_g h$,可以通过如下步骤将问题约化为素数 p_i 阶循环群上的离散对数求解。

首先,利用孙子定理,可以将求解 $x \bmod N$ 转化为求解 $x \bmod p_i^{e_i}, 1 \leqslant i \leqslant n$,从而问题转化为阶为素数幂循环群的离散对数求解。

其次,可以将阶为素数幂的离散对数求解转化为阶为素数的离散对数求解。例如,为了求解 $x_1 = x \bmod p_1^{e_1}$,不妨假设 $x_1 = c_0 + c_1 p_1 + \cdots + c_{e_1-1} p_1^{e_1-1}$,其中,$0 \leqslant c_i \leqslant p-1$。记 $g_0 = g^{N/p_1^{e_1}}$, $h_0 = h^{N/p_1^{e_1}}$,则 g_0 生成一个阶为 $p_1^{e_1}$ 的循环子群,$h_0 = g_0^{x_1}$。令 $g_1 = g_0^{p_1^{e_1-1}}$,$h_1 = h_0^{p_1^{e_1-1}}$,则 g_1 生成一个阶为 p_1 的循环子群, $c_0 = \log_{g_1} h_1$ 可以由穷搜或者结合接下来介绍的通用算法求解。进一步,令 $h_1 = h_0 g_0^{-c_0}$,则 $c_1 = \log_{g_1} h_1^{p_1^{e_1-2}}$。其余 c_i 类似可得。

2.4 小步-大步法

Shanks[28]利用时间-空间折中的思想设计了求解离散对数的小步-大步法,该方法是确定性求解算法,而且渐进复杂度优于穷搜法。

记 $m = \lceil \sqrt{N} \rceil$,利用带余除法,可以将待求的离散对数写成

$$x = am + b, 0 \leqslant a, b < m,$$

为了求解对应的 a, b,注意到有等式(碰撞)

$$g^b = hg^{-am}。$$

可以通过寻找碰撞的方法求解。首先,计算 $(b, g^b), 0 \leqslant b < m$ 并存储在一个排序的列表中(可以存储在二元树、哈希表,或者存储后排序)。然后,计算 (a, hg^{-am}) 并判断是否和上一个列表中的

元素重复(即发生碰撞)。找到碰撞之后,可以通过对应的(a,b)恢复离散对数。

小步-大步法的时间和空间复杂度为$\widetilde{O}(\sqrt{N})$,其中,$\widetilde{O}(f)=O(f\log^c f)$,$c$ 为一个常数。一些研究者尝试构造多个形如$\{g^{a_i}h^{b_i}\}$的列表以提高寻找碰撞的效率[29-30]。

2.5　低存储的概率算法

为了降低空间复杂度,可以采用伪随机游走等方法设计概率求解算法。

2.5.1　Pollard Rho 方法

针对基本的离散对数问题,Pollard[31]基于生日碰撞的思想设计了 Rho 方法。假设找到碰撞

$$g^{a_1}h^{b_1}=g^{a_2}h^{b_2},$$

从而

$$(b_1-b_2)x\equiv a_2-a_1(\bmod N)。$$

如果$gcd(b_1,b_2,N)=1$,那么可以求解 x。

为了能够以较低的空间找到所需的碰撞,Rho 方法结合了伪随机游走和 Floyd 寻找碰撞的技术。Pollard 将 G 划分成 3 个互不相交的集合 G_1,G_2,G_3。选定初始值$s_0=g^{a_0}h^{b_0}$,定义如下伪随机游走序列$s_i=g^{a_i}h^{b_i}$,

$$s_{i+1}=f(s_i)=\begin{cases}s_i^2, s_i\in G_0\\ gs_i, s_i\in G_1\\ hs_i, s_i\in G_2\end{cases},$$

对应的可以得到(a_{i+1},b_{i+1})的迭代公式。为了找到碰撞$s_m=s_n$,$m\neq n$,在第 i 步保存信息$(s_i,a_i,b_i,s_{2i},a_{2i},b_{2i})$并判断是否$s_i=s_{2i}$。

Rho 算法的分析在启发式假设下采用了生日碰撞问题的结论,算法的平均时间复杂度为$O(\sqrt{N})$次群运算,空间复杂度为$O(1)$。

研究者后续提出了针对 Rho 方法的许多改进,包括采用并行计算、群的划分以及使用其他形式的随机游走等。

Kuhn 等[32]推广了 Rho 方法求解 L 个目标元素的离散对数,算法复杂度为$O(\sqrt{LN})$。

2.5.2　Pollard 袋鼠算法与 Gaudry-Schost 方法

针对小区间离散对数问题$0\leqslant x<N$,Pollard[31]提出了袋鼠算法,也称 Lambda 方法。

在袋鼠算法中有 2 类游走,一类是家袋鼠游走g^{a_i},另一类是野袋鼠游走hg^{b_i}。与 Rho 方法中的游走类似的是,Lambda 方法中袋鼠的游走是由现在的值所对应的分类决定;不同的是,步长按照预计算的一些小步决定。

Lambda 方法的分析不是基于生日碰撞问题,而是基于其他概率分析,其复杂度为$O(\sqrt{N})$。

Van Oorschot 和 Wiener 使用了区分点技术来降低存储,王瑶等[33]通过将一次大整数乘法分解为多次小整数乘法提高运算效率。

针对高维离散对数问题,Gaudry 等[34]用伪随机游走结合区分点的算法。

区分点是一些预先设定的具有良好的统计性质但又可以高效检验的元素。Gaudry-Schost 算法求解高维离散对数的时候,先随机选取一个起始点,然后采用随机游走,到达某一区分点后记录信息,最后重新开始新的随机游走。当 2 个不同类型的游走(形如g^{a_i}和hg^{b_i})达到同一区分点时(发生碰撞),即可以计算出所求的离散对数。该算法的复杂度与 Lambda 方法类似,均为$O(\sqrt{N})$,其中,N 为搜索空间大小。

目前,计算 1 维区间上离散对数问题的最快方法由 Galbraith 等[35]提出,他们分别利用 4 个袋鼠和调节碰撞区间加速了 Lambda 方法和 Gaudry-Schost 算法。算法复杂度仍为$O(\sqrt{N})$级别,在前面的系数上有所改进。

2.6　一般群模型和计算下界

上述算法没有利用群的任何其他性质,因此,对所有抽象群都适用。

为了刻画求解离散对数问题求解的复杂度下界,研究者提出了带有限制的模型。Nechaev[36]和 Shoup[37]各自提出通用群模型,在通用群模型下证明了求解阶为 N 的离散对数问题的通用算法复杂度为$\Omega(\sqrt{p})$,其中,p 为整除 N 的最大素因子。

Yun[38]证实了 Kuhn 和 Struik 关于一般群模型下求解多个目标元素离散对数复杂度的下界,即求解 L 个目标元素的离散对数,算法复杂度为$O(\sqrt{Lp})$。

Bartusek 等[39]指出在通用群模型下,群的生成元是固定的,或者是随机影响到离散对数问题和 DH 问题的求解下界。

3　指标计算框架

根据上述结论可知,为降低算法复杂度的数量级,需要利用群的具体特性。注意到,离散对数

满足如下等式:

$$\log_g(h_1h_2)=\log_g(h_1)+\log_g(h_2)。$$

该性质启发我们求解离散对数的时候,不止需要考察元素本身,也需要考察元素的分解情况。如果能赋予群元素一种"大小"关系,并且能够用某种方法将"较大"元素表示成"较小"元素的乘积,那么就可以从"较小"元素的离散对数恢复出"较大"元素的离散对数。特别地,当群中的元素可以自然地看成(代数)整数或者有限域上的多项式时,可以用范数或多项式的次数来描述元素的大小关系。

上述思想已经体现在早期相关的工作中,并逐步发展完善,基于上述基本思想设计了指标计算框架,应用于整数分解、有限域和超椭圆曲线离散对数求解等。而对于椭圆曲线,目前暂未找到比较好的指标计算方法。

3.1 光滑性和概率

指标计算方法中的一个基本概念是(在合适范数下的)光滑性,其刻画一个"较大"元素是否能表示成一些"较小"元素的乘积。

一个整数 $m=\prod_{i=1}^{s}p_i^{e_i}$ 称为 n - 光滑,如果对任意的 $1\leqslant i\leqslant s$,都有 $p_i\leqslant n$。一个有限域上的多项式 $f(x)\in\mathbb{F}_q[x]$ 称为 d - 光滑,如果 $f(x)$ 的所有不可约因子的次数不超过 d。

Canfield 等[40]研究了整数光滑的概率。当参数 a 充分大的时候,不超过 a 的所有正整数是 b - 光滑的概率是 $u^{-u+o(1)}$,其中,$u=\frac{\log a}{\log b}$。

Odlyzko[41]以及 Panario 等[42]分析了有限域上多项式光滑的概率。当 k 充分大的时候,次数不超过 k 的所有多项式 d - 光滑的概率是 $u^{-u+o(1)}$,其中,$u=\frac{k}{d}$。

3.2 指标计算框架

指标计算框架一般包括如下 3 个部分:

(1)确定因子基(也称光滑基)。根据具体的问题参数确定因子基 $S=\{s_1,s_2,\cdots,s_k\}\subset G$,例如,选定光滑界 b 之后所有 b - 光滑的元素添加 g 的集合。

(2)求解因子基元素离散对数。首先需要生成关系式,考察同态映射:

$$\varphi:\mathbb{Z}^k\to G,$$

其中,$\varphi(x_1,\cdots,x_k)=s_1^{e_1}\cdots s_k^{e_k}$。映射的核是:

$$\ker(\varphi)=\{(x_1,\cdots,x_k)\mid s_1^{e_1}\cdots s_k^{e_k}=1\}$$

生成因子基元素之间的一个关系式就是通过一定的方法找到核空间中的一个元素 $(e_{11},\cdots,e_{1k})$ 对应的等式 $s_1^{e_{11}}\cdots s_k^{e_{1k}}=1$,两边取对数得:

$$e_{11}\log_g s_1+\cdots+e_{1k}\log_g s_k=0\bmod N。$$

因此,通过关系式就得到了一个以因子基元素离散对数为变量的线性同余方程。

当收集到足够多的关系式,就可以求解线性同余方程组,得到因子(后面都统一成因子基)基元素的离散对数。

在实际求解过程中,所得到线性同余方程往往是稀疏的,可以采用比消元法更快的求解算法,如 Wiedemann 算法[43]。

(3)目标元素离散对数。给定目标元素 h,为了求解这个元素的离散对数,可以通过一定的方法将该元素(可以是该元素的方幂)表示为因子基元素的组合。从而可以由因子基元素的离散对数推导出目标元素的离散对数。

4 有限域离散对数求解

有限域上的任意函数可以表示称为多项式的形式,特别地,有限域上的离散对数看作一个函数也有多项式表示[44-49],但是直接使用多项式计算离散对数的效率并不高。

针对有限域的具体表示,可以结合指标计算框架设计比通用求解算法更高效的方法,记 $L_Q(\alpha,c)=\exp((c+o(1))(\log Q)^{\alpha}(\log\log Q)^{1-\alpha})$,其中,$0\leqslant\alpha\leqslant1$,$c$ 是一个常数,有时简记为 $L_Q(\alpha)$ 或者 $L(\alpha)$。

4.1 有限域按照特征的分类

令 $Q=p^n$ 表示有限域 $\mathbb{F}_{p^n}$ 的元素个数,考虑当参数趋于无穷的情况,随着 $Q\to\infty$ 特征 $p=L_Q(\alpha_p,c_p)$。

如果 $\alpha_p>1/3$,称为中等特征或大特征有限域,目前最快的求解算法是数域筛法[50-53],时间复杂度是亚指数时间;如果 $\alpha_p<1/3$,称为小特征的情况,目前最快的求解算法渐进时间复杂度为准多项式时间[54-57]。

4.2 中等和大特征有限域离散对数

数域筛法是在指标计算框架的基础上,结合

中等和大特征有限域的具体表示设计的,其将有限域提升到数域中,利用数域中元素的范数来确定元素的大小。数域筛法包括多项式选取、因子基离散对数求解和目标元素离散对数求解。设目标有限域为$\mathbb{F}_{p^n}$。

(1)在多项式选取阶段,需要选取 2 个整系数的不可约多项式$f(x)$和$g(x)$,使得它们的模 p 有 n 次不可约公因式$\psi(x)$。这样可以得到$\mathbb{Q}$上的 2 个数域 K_f 和 K_g,如图 1 所示。

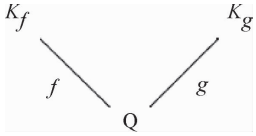

图 1　数域构造

Fig. 1　Construction of number fields

并且有限域$\mathbb{F}_{p^n}=\mathbb{F}_p[x]/(\psi(x))$可以分别自然地提升到 K_f 和 K_g 的子环$\mathbb{Z}[x]/f(x)$和$\mathbb{Z}[x]/g(x)$中,如图 2 所示。

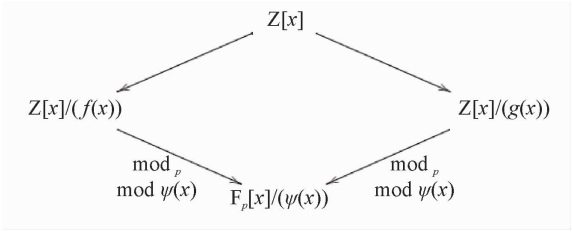

图 2　数域筛法

Fig. 2　The number field sieve

对于一个整系数多项式,可以分别将其看成 K_f 和 K_g 中的元素,并且通过有限域$\mathbb{F}_{p^n}$联系起来。

(2)在因子基元素离散对数阶段,需要根据具体参数选取合适的因子基,通过筛法求解出相应的离散对数。

由于数域中只存在素理想的唯一分解,因此,取因子基为一些范数较小的素理想。这里以筛 1 次多项式为例,此时取因子基为范数不超过 B 的 1 次素理想。

在给定范围内筛(a,b)对,希望多项式 $a+bx$ 在 K_f 和 K_g 中同时 B - 光滑,即 $a+bx$ 在 K_f 和 K_g 中生成的主理想能同时分解成因子基中素理想的乘积。这样便得到了因子基元素之间的一个同余方程。接着利用 λ 映射[51],将素理想之间的关系方程转化成元素之间的关系方程。当得到足够多的关系方程后,通过解方程便可得到因子基元素的离散对数。

需要注意的是,对于中等特征有限域,通常筛 1 次多项式是不够的,还需要筛高次多项式。此时因子基也需要包含相应的高次素理想。

(3)在目标元素离散对数求解阶段,需要在前 2 步的基础上求解给定的目标元素离散对数。这一步又可以分为 2 个阶段:光滑化阶段和递降阶段。

在光滑化阶段,通过将目标元素随机化,期待其较为光滑,即希望目标元素能分解成若干范数较小的元素。在递降阶段,将上述范数较小的元素通过格筛的方法进一步降低其范数,使其归约到因子基元素中,从而恢复出对应的离散对数。

数域筛法的渐进复杂度为 $L(1/3,c)$,在实际使用中,计算因子基离散对数是其最耗时的部分。目前,数域筛法的改进均集中在第二个参数 c 上。

由于数域定义多项式的性质将影响被筛元素的光滑概率,从而影响算法的复杂度,研究者提出了多种不同的多项式选取方法[52,58-60]。特别地,当有限域的特征满足某些特定条件时,可以构造出性质更好的多项式,这类方法称为特殊数域筛法[61-62]。

有别于仅构造 2 个数域,研究者发现可以利用多个数域提高关系方程的收集效率,这类方法称为多重数域筛法[63-65]。

经典数域筛法是构造有理数域$\mathbb{Q}$上的 2 个数域。如果将基域$\mathbb{Q}$换成一个代数数域,此时,可以给出(扩展)数域塔筛法[53,66]。该方法可以降低中等特征有限域离散对数的求解复杂度。

如果构造的数域具有非平凡的自同构,可以利用自同构将因子基中元素划分成等价类,从而减少所需计算的因子基离散对数数目[52,59]。

当有限域的扩张次数大于 1 时,可以利用有限域的真子域构造范数较小的等价元素,以提高目标元素的光滑概率,从而降低光滑化阶段的复杂度[67-69]。

在递降阶段,除了常用的一次素理想外,也可以使用高次素理想来提高计算效率[69-70]。

目前,计算素域中离散对数的记录由 Boudot 等[71]保持,他们使用数域筛法计算了整数模 795 比特安全素数的素域中的离散对数问题。值得注意的是,Fried 等[72]在此之前计算了 1 024 比特素域中的离散对数,不过这里选取的素域适用于特

殊数域筛法,并且其有160比特的子群。

4.3 小特征有限域离散对数

早期求解小特征有限域离散对数较快的算法是在指标计算框架基础上发展出的函数域筛法[73-76]。函数域筛法与数域筛法类似,只不过将有限域提升到函数域,用多项式的次数代替之前数域中元素的范数来确定元素的大小。

原始的函数域筛法过于技术性,Joux等[76]在2006年给出了简化版本。算法的框架如图3所示:

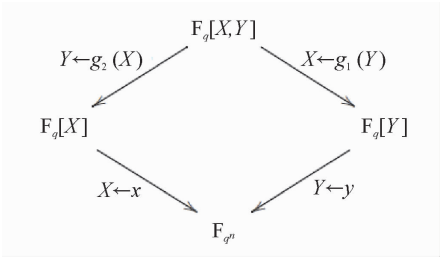

图3 函数域筛法

Fig. 3 The function field sieve

函数域筛法的流程与数域筛法类似,不同的是,此时处理对象是函数域中的多项式而不是数域中的代数整数,这里省略算法细节。

在2013年,Joux[77]提出了小特征有限域的Frobenius表示,并且提出了复杂度为$L(1/4)$的求解算法。此后又进一步改进得到准多项式时间的BGJT算法。

下面简要描述给定小特征有限域$\mathbb{F}_{p^k}$应用BGJT算法求解对应离散对数的基本步骤:

(1)构造有限域的Frobenius表示。为此,需要将给定的有限域嵌入到合适的扩域:

$$\mathbb{F}_{p^k} \rightarrow \mathbb{F}_{q^k} \rightarrow \mathbb{F}_{q^{2k}},$$

这里,$q = p^r$, $r = \lceil \log_p k \rceil$。

搜索低次数多项式$h_0, h_1 \in \mathbb{F}_{q^2}[x]$使得存在不可约因子:

$$f(x) \mid h_1(x)x^q - h_0(x),$$

其中,$f(x) \in \mathbb{F}_{q^2}[x]$,并且$\deg(f(x)) = k$。

令$\mathbb{F}_{q^{2k}} = \mathbb{F}_{q^2}[\zeta]$,这里$\zeta$是$f(x)$的一个根,这样就得到了有限域的一个Frobenius表示。这种表示下有:

$$\zeta^q = \frac{h_0(\zeta)}{h_1(\zeta)},$$

该性质有利于提高后续产生关系式的效率。但是,Cheng等[78]指出采用这种表示本质上是在剩余类环$\mathbb{F}_{q^2}[x]/(h_1(x)x^q - h_0(x))$上做运算,需要处理零因子的影响。

(2)假设选取相对于ζ次数为1的有限域元素为因子基元素。为了求解因子基元素的离散对数,注意到有恒等式:

$$\prod_{\alpha \in \mathbb{F}_q} (x - \alpha) = x^q - x,$$

应用Mobius变换

$$x \mapsto \frac{a\zeta + b}{c\zeta + d},$$

其中,$(a,b,c,d) \in \mathbb{F}_{q^2}^4$并且$ad - bc \neq 0$,得到

$$\prod_{\alpha \in \mathbb{F}_q} \frac{(a - \alpha c)\zeta + (b - \alpha d)}{(c\zeta + d)^q} = \frac{(c\zeta + d)(a\zeta + b)^q - (a\zeta + b)(c\zeta + d)^q}{(c\zeta + d)^{q+1}},$$

去掉分母后得到

$$(c\zeta + d)\prod_{\alpha \in \mathbb{F}_q}((a - \alpha c)\zeta + (b - \alpha d)) = (c\zeta + d)(a\zeta + b)^q - (a\zeta + b)(c\zeta + d)^q。$$

根据q-次方幂的性质得到

$$(c\zeta + d)\prod_{\alpha \in \mathbb{F}_q}((a - \alpha c)\zeta + (b - \alpha d)) = (c\zeta + d)(a^q\zeta^q + b^q) - (a\zeta + b)(c^q\zeta^q + d^q)。$$

根据构造有$\zeta^q = h_0(\zeta)/h_1(\zeta)$,带入上式得

$$h_1(\zeta)(c\zeta + d)\prod_{\alpha \in \mathbb{F}_q}((a - \alpha c)\zeta + (b - \alpha d)) = (a^q h_0(\zeta) + b^q h_1(\zeta))(c\zeta + d) - (a\zeta + b)(c^q h_0(\zeta) + d^q h_1(\zeta))。$$

注意到上式2边相对于ζ的次数都不高,因此有较高的概率2边都分裂成一次元素的乘积。

为了得到不同的关系式,需要选取子群$PGL(2, q)$在群$PGL(2, q^2)$中不同陪集的代表元[79]。

(3)假设目标元素是$W(\zeta) \in \mathbb{F}_{q^{2k}}[\zeta]$, W相对于ζ的次数大于1。

类似地,考虑恒等式:

$$\prod_{\alpha \in \mathbb{F}_q} (x - \alpha) = x^q - x,$$

然后应用变量替换

$$x \mapsto \frac{aW(x) + b}{cW(x) + d},$$

带入并展开后可得左边是W相关的元素乘积,如果右边是$\deg(W)/2$光滑的,就得到一个关系式。收集到足够多的关系式之后,可以将W约化到$\deg(W)/2$光滑的元素。通过迭代,可以归约到因子基元素的离散对数。

针对小特征有限域离散对数时间复杂度较低

的求解算法有的依赖于一些启发式假设,一些改进工作旨在探索是否可以减少或者替换启发式假设,比如概率算法[57]和确定性算法[80]。

目前,小特征有限域离散对数的计算记录由 Granger 等[81]保持,他们求解了 30 750 比特二元域中的离散对数。

5　椭圆曲线离散对数求解

给定定义在有限域$\mathbb{F}_q$上的椭圆曲线 E,$\mathbb{F}_q$有理点 P,Q,椭圆曲线离散对数问题[82-83]是求解最小整数 x,使得 $Q=xP$。实际使用一般是基于一个阶数比较大的循环子群。该问题是椭圆曲线密码学安全性的基石,在双线性对密码学中也是安全性基础之一。

根据 Hasse 定理,定义在$\mathbb{F}_q$上椭圆曲线有理点的个数 N_E 满足

$$q+1-2\sqrt{q}\leqslant N_E\leqslant q+1+2\sqrt{q},$$

其中,$q+1-N_E$ 称为 E 的迹。

5.1　一般椭圆曲线

针对一般的椭圆曲线离散对数问题,目前通用求解方法仍是最优的计算椭圆曲线离散对数的方法。为了减少空间复杂度,经常采用的是基于伪随机游走的方法,例如,Pollard 方法和 Gaudry-Schost 方法等。李俊全等[84]研究了迭代函数的设计准则,并且给出了一个改进的并行碰撞算法。

但是结合椭圆曲线的性质,可以做一些改进。例如,Gallant 等[85]和 Wiener 等[86]提出利用自同构将群元素划分成等价类,从而提高算法效率。Galbraith 等[87]利用椭圆曲线易于求逆的性质对区间离散对数求解进行加速,Zhu 等[88]在此基础上进一步做出了改进。Zhang 等[89]用二元域上椭圆曲线的半点运算比倍点运算更快的特点加速离散对数的求解。Wu 等[90]给出了 Gaudry-Schost 算法的一个渐近时间复杂度最优的改进.

5.2　归约到有限域

5.2.1　归约到有限域乘法群

Meneze 等[91]和 Frey 等[92]利用双线性映射工具提出了一种约化方法,将椭圆曲线离散对数问题归约到有限域的适当扩域$\mathbb{F}_{q^k}$上的离散对数问题,然后利用计算有限域离散对数的更高效的求解方法。这里的 k 称为曲线的嵌入次数,其通常很大,因此该方法仅对少数曲线有效。特别地,当曲线的迹被 p 整除时,这类曲线称为超奇异椭圆曲线,其嵌入次数不超过 6,极易受到这类方法攻击。

针对特殊的参数,文献[93-94]考察了有限域离散对数问题和椭圆曲线离散对数问题的关系。

5.2.2　归约到有限域加法群

如果椭圆曲线满足 $N_E=q$,即迹为 1,称为异常椭圆曲线。特别地,当 $q=p$ 为素数时,这类曲线的点群恰好是素数阶的,似乎满足密码学的要求。但是异常椭圆曲线离散对数问题却是十分容易的,Smart[95]、Satoh 等[96]、Semaev[97]分别独立给出了高效求解算法。前 2 者是一种提升方法,针对素域的情形,将曲线提升到 p 进数域$\mathbb{Q}_p$中,利用形式对数将椭圆曲线的点群归约成有限域的加法群。之后朱玉清等[98]拓展了提升方法的使用范围,可以求解一般有限域上椭圆曲线p-群中的离散对数问题。Semaev 则是利用除子和微分形式空间的对应,在固定点的取值将椭圆曲线离散对数问题归约成有限域加法群中的离散对数问题。之后祝跃飞等[99]对其进行优化,给出了在无穷远点取值的方法,避免了在扩域上进行运算。

5.3　归约到高亏格曲线

在椭圆曲线上直接设计指标计算法并不容易(见下一小节),但对于亏格 $g\geqslant 2$ 的光滑代数曲线 C,存在指标计算法可以有效地计算其雅可比 Jac(C)中的离散对数。当曲线是超椭圆曲线时,由于其雅可比中元素存在 Mumford 表示,即表示成 2 个次数较低的多项式,利用多项式的分解性质可以给出亚指数时间的指标计算法[100]。对于一般曲线,研究者利用“双大素数”技巧给出了时间复杂度为 $O(q^{2-2/g})$的算法,即使对于较小的亏格 g,其效率也优于 Pollard rho 算法[101-102]。

为了利用上述指标计算法,自然的想法是将椭圆曲线离散对数归约成代数曲线雅可比中的离散对数。为此,Frey 等[103]提出了 Weil 下降方法,之后 Galbraith 等[104]对其进行了完善。

设 E 是定义在扩域$\mathbb{F}_{q^n}$上的椭圆曲线,曲线方程为$f(X,Y)=0$。取$\mathbb{F}_{q^n}$关于$\mathbb{F}_q$的一组基$\{1,\theta,\theta^2,\cdots,\theta^{n-1}\}$,令

$$X=X_0+X_1\theta+\cdots+X_{n-1}\theta^{n-1},$$

$$Y=Y_0+Y_1\theta+\cdots+Y_{n-1}\theta^{n-1},$$

则$f(X,Y)=0$ 可以表示成

$$\sum f_i(X_0,\cdots,X_{n-1},Y_0,\cdots,Y_{n-1})\theta^i = 0,$$

其中,f_i 是 $\mathbb{F}_q$ 上多项式。通过这种方式,可以由 $\mathbb{F}_{q^n}$ 的椭圆曲线得到 $\mathbb{F}_q$ 上的 n 维阿贝尔簇。如果能找到一条曲线 C 使得其雅可比 Jac(C) 包含该阿贝尔簇,则能将椭圆曲线的离散对数问题归约成 Jac(C) 中的离散对数问题,再利用指标计算法求解。

对于特征 2 有限域,Gaudry 等[105]利用函数域的 Artin-Schreier 扩张构造了满足条件的曲线,之后 Diem[106]用 Kummer 扩张给出了奇特征情形的构造方式,这类构造方法统称为 GHS 攻击。该攻击对一些曲线取得了比较好的效果,但是对于大部分椭圆曲线而言,该方法得到的覆盖曲线的亏格很高,其关于 n 是指数级的,导致效率并不比通用算法高。

5.4 基于求和多项式的指标计算法

仿照第 3 节指标计算法的框架,椭圆曲线离散对数的指标计算流程如下:取定 $E(\mathbb{F}_q)$ 的某个子集为因子基;选取随机的点 $R = aP + bQ$,将其分解成因子基中点的和,即 $aP + bQ = \sum e_iP_i$,其中,P_i 为因子基中元素;收集足够多这样的关系式,从而计算出 Q 关于 P 的离散对数。

对于有限域中的元素,其可以自然地提升到数域或者函数域,根据素理想或者多项式的唯一分解性可以分解成一些范数小或者次数低的元素。而对于椭圆曲线,如何定义因子基并给出有效的点分解算法是设计椭圆曲线指标计算法的难点所在。为此,Semaev[107]提出了求和多项式。

设 E 是定义在域 K 上的椭圆曲线,定义 m 次求和多项式 $S_m(X_1,X_2,\cdots,X_m)$ 为满足如下性质的多项式:令 $x_1,x_2,\cdots,x_m$ 为 K 的代数闭包 $\overline{K}$ 中的 m 个元素,$S_m(x_1,x_2,\cdots,x_m)=0$ 当且仅当存在 $y_1,y_2,\cdots,y_m$ 使得 $(x_i,y_i)\in E(\overline{K})$,并且

$$(x_1,y_1)+(x_2,y_2)+\cdots+(x_m,y_m)=O,$$

其中,O 是 $E(\overline{K})$ 的无穷远点。求和多项式序列 $\{S_m\}$ 可以递归地构造,其次数增长是指数级的。

对于素域上的椭圆曲线,一般取因子基为 x 坐标小于预先取定的正整数 B 的有理点全体。此时,为了得到点 $R=(x_R,y_R)$ 与因子基元素的关系式,可以计算 $S_m(X_1,X_2,\cdots,X_{m-1},x_R)=0$ 中小于 B 的零点。若该方程存在零点,则说明可以找到点 R 与 $m-1$ 个因子基元素的关系式。对于扩域 $\mathbb{F}_{q^n}$ 上的椭圆曲线,Gaudry[108]和 Diem[109]取因子基为 x 坐标落在 $\mathbb{F}_{q^n}$ 的某个 $\mathbb{F}_q$ 子空间中的有理点全体。通过对 $S_m=0$ 使用 Weil 限制,可以将 $\mathbb{F}_{q^n}$ 上的方程转换成子域 $\mathbb{F}_q$ 上 n 个代数方程,从而更易于计算。

然而计算上述代数方程(组)的零点通常并不容易,一般均需使用 Gröbner 基算法,算法的时间复杂度为 $O(N^d)$,其中,N 为变量个数,d 为正则次数。研究表明,这类方程的正则次数通常很高[110-111]。

为了提高求解求和多项式零点的效率,研究者尝试利用求和多项式的对称性降低多项式的次数[112-113],将求和多项式分裂成多个子求和多项式组,通过增加变量数目降低方程次数[114],以及利用 Frobenius 映射加速方程的求解[115]。

参考文献:

[1] Lidl R, Niederreiter H. Finite fields[M]. 2nd Edition. Cambridge: Cambridge University Press, 2000.

[2] Mukund S K, Rao T R N, Zeng K C. On reducing test length in LFSR based testing[C]//VLSI Design 1991. Piscataway: IEEE, 1991: 231-236.

[3] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[4] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

[5] Diffie W, Oorschot P, Wiener M. Authentication and authenticated key exchanges[J]. Designs Codes and Cryptography, 1992, 2(2): 107-125.

[6] 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.

[7] Schnorr C. Efficient identification and signatures for smart cards[C]//Eurocrypt. Berlin: Springer, 1989: 688-689.

[8] National Institue of Standards and Technology. Digital signature standard[S]. FIPS Publication 186, 1994.

[9] Melchor C A, et al. NIST post-quantum cryptography standardization round 2 submission: Hamming quasi-cyclic (HQC). http://pqc-hqc.org/.
[10] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings[C]//Eurocrypt. Berlin: Springer, 2010: 1-23.
[11] 曹珍富. Z[ω]环上的两类密码体制[J]. 电子科学学刊, 1992, 14(3): 286-290.
[12] Miller V. Use of elliptic curves in cryptography[C]//Crypto. Berlin: Springer, 1986: 417-426.
[13] Koblitz N. Ellitpic curve cryptosystems[J]. Mathematics of Computation, 1987, 48: 203-209.
[14] Brands S. An efficient off-line electronic cash system based on the representation problem[R]. CS-R9323, CWI, 1993.
[15] Döttling N, Garg S. Identity-based encryption from the Diffie-Hellman assumption[C]//Crypto. Berlin: Springer, 2017: 537-569.
[16] Garg S, Hajiabadi M. Trapdoor functions from the computational Diffie-Hellman assumption[C]//Crypto. Berlin: Springer, 2018: 362-391.
[17] Micheli G, Gaudry P, Pierrot C. Asymptotic complexities of discrete logarithms in pairing-relevant finite fields[C]//Crypto. Berlin:Springer, 2020: 32-61.
[18] Joux A. A one round protocol for tripartite Diffie-Hellman[J]. Journal of Cryptology, 2004, 17(4): 263-276.
[19] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[J]. SIAM Journal on Computating, 2003, 32(3): 586-615.
[20] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[J]. Journal of Cryptology, 2004, 17: 297-319.
[21] Boneh D, Schacham H. Group signatures with verifier-local revocation[C]//CCS. New York:ACM, 2004: 168-177.
[22] Boneh D, Silverberg A. Applications of multilinear forms to cryptography[J]. Contemporary Mathematics, 2003, 324: 71-90.
[23] Abadi M, Feigenbaum J, Kilian J. On hiding information from an oracle[J]. Journal of Computer and System Sciences, 1989, 39(1): 21-50.
[24] Hastad J, Naslund M. The security of all RSA and discrete log bits[J]. Journal of the ACM, 2004, 51(2):187-230.
[25] Shor P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computing, 1997, 26(5): 1484-1509.
[26] Kitaev A. Quantum measurements and the Abelian stabilizer problem[DB/OL](1995-11-20). http://arxiv.org/abs/quant-ph/9511026
[27] Pohlig S, Hellman M. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance[J]. IEEE Transactions on Information Theory, 1978, 24(1): 106-110.
[28] Shanks D. Class number, a theory of factorization and genera[C]//Proceedings of Symposia in Pure Mathematics. New York:AMS, 1971: 415-440.
[29] Chateauneuf M, Ling A, Stinson D. Slope packings and coverings, and generic algorithms for the discrete logarithm problem [J]. Journal of Combinatorial Designs, 2003, 11(1): 36-50.
[30] Bernstein D, Lange T. Two grumpy giants and a baby[C]//Proceedings of the Tenth Algorithmic Number Theory Symposium. Berkely: Mathematical Sciences Publishers,2013: 321-340.
[31] Pollard J. Monto Carlo methods for index computations (mod p)[J]. Mathematics of Computation, 1978, 32: 918-924.
[32] Kuhn F, Struik R. Random walks revisited: Extensions of pollard's Rho algorithm for computing multiple discrete logarithms [C]//SAC. Berlin:Springer, 2001: 212-229.
[33] 王瑶,吕克伟. 关于区间上离散对数问题的改进算法[J]. 密码学报,2015, 2(6):570-582.
[34] Gaudry P, Schost E. A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm[C]//Ants. Berlin: Springer, 2004: 208-222.
[35] Galbraith S, Pollard J, Ruprai R. Computing discrete logarithms in an interval[J]. Mathematics of Computation, 2013, 82(282): 1181-1195.
[36] Nechaev V I. Complexity of a determinate algorithm for the discrete logarithm[J]. Mathematical Notes, 1994, 55(2): 165-172.
[37] Shoup V. Lower bounds for discrete logarithm and related problems[C]//Eurocrypt. Berlin: Springer, 1997: 256-266.
[38] Yun A. Generic hardness of the multiple discrete logarithm problem[C]//Eurocrypt. Berlin: Springer, 2015: 817-836.

[39] Bartusek J, Ma F, Zhandry M. The distinction between fixed and random generators in group-based assumptions[C]// Crypto. Berlin: Springer, 2019: 801-830.

[40] Canfield E R, Erdös P, Pomerance C. On a problem of Oppenheim concerning "factorisatio numerorum"[J]. Journal of Number Theory, 1983, 17: 1-28.

[41] Odlyzko A M. Discrete logarithm in finite fields and their cryptographic significance[C]//Eurocrypt 1984. Berlin: Springer, 1985: 224-314.

[42] Panario D, Gourdon X, Flajolet P. An analytic approach to smooth polynomials over finite fields[C]//ANTS. Berlin: Springer, 1998: 226-236.

[43] Wiedemann D H. Solving sparse linear equations over finite fields[J]. IEEE Transactions on Information Theory, 1986, 32(1): 54-62.

[44] Wells A Jr. A polynomial form for logarithms modulo a prime[J]. IEEE Transactions on Information Theory, 1984, 30(6): 845-846.

[45] Mullen G, White D. A polynomial representation for logarithms in GF(q)[J]. Acta Arithmetica, 1986, 47(3): 255-261.

[46] Niederreiter H. A short proof for explicit formulas for discrete logarithms in finite fields[J]. Applicable Algebra in Engineering, Communication and Computing, 1990, 1(1): 55-57.

[47] Meletiou G, Mullen G. A note on discrete logarithms in finite fields[J]. Applicable Algebra in Engineering, Communication and Computing, 1992, 3: 75-78.

[48] Winterhof A. Polynomial interpolation of the discrete logarithm[J]. Designs Codes and Cryptography, 2002, 25: 63-72.

[49] Wan Z X. A short proof for an explicit formula for discrete logarithms in finite fields[J]. Discrete Mathematics, 2008, 308(21): 4914-4915.

[50] Gordon D M. Discrete logarithms in GF(p) using the number field sieve[J]. SIAM Journal on Discrete Mathematics, 1993, 6(1): 124-138.

[51] Schirokauer O. Discrete logarithms and local units[J]. Philosophical Transactions of the Royal Society A, 1993, 345(1676): 409-423

[52] Joux A, Lercier R, Smart N, et al. The number fields sieve in the medium prime case[C]//Crypto. Berlin: Springer, 2006: 326-344.

[53] Kim T, Barbulescu R. Extended tower number field sieve: A new complexity for the medium prime case[C]//Crypto. Berlin: Springer, 2016: 543-571

[54] Barbulescu R, Gaudry P, Joux A, et al. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic[C]//Eurocrypt. Berlin: Springer, 2014: 1-16.

[55] Joux A, Pierrot C. Technical history of discrete logarithms in small characteristic finite fields: The road from subexponential to quasi-polynomial complexity[J]. Designs, Codes and Cryptography, 2016, 78: 73-85.

[56] Granger R, Kleinjung T, Zumbrägel J. Indiscreet logarithms in finite fields of small characteristic[J]. Advances in Mathematics of Communications, 2018, 12(2): 263-286.

[57] Granger R, Kleinjung T, Zumbräger J. On the discrete logarithm problem in finite fields of fixed characteristic[J]. Transactions of the American Mathematical Society, 2018, 370: 3129-3145.

[58] Matyukhin D. Effective version of the number field sieve for discrete logarithm in a field GF(p^k)[J]. Trudy po Diskretnoi Matematike, 2006, 9: 121-151.

[59] Barbulescu R, Gaudry P, Guillevic A, et al. Improving NFS for the discrete logarithm problem in non-prime finite fields[C]//Eurocrypt 2015. Berlin: Springer, 2015: 115-129.

[60] Sarkar P, Singh S. New complexity trade-offs for the (multiple) number field sieve algorithm in non-prime fields[C]//Eurocrypt. Berlin:Springer, 2016: 429-458.

[61] Semaev I. Special prime numbers and discrete logs in finite prime fields[J]. Mathematics of Computation, 2002, 71(237):363-377.

[62] Joux A, Pierrot C. The special number field sieve in F_{p^n}, Application to pairing-friendly constructions[C]//Pairing 2013. Berlin:Springer, 2013: 45-61.

[63] Matyukhin D. On asymptotic complexity of computing discrete logarithms over GF(p)[J]. Discrete Mathematics and Applications dma, 2003, 13(1): 27-50.

[64] Barbulescu R, Pierrot C. The multiple number field sieve for medium-and high-characteristic finite fields[J]. LMS Journal of Computation and Mathematics, 2014, 17: 230-246.

[65] Pierrot C. The multiple number field sieve with Conjugation and Generalized Joux-Lercier methods[C]//Eurocrypt 2015. Berlin: Springer, 2015: 156-170.

[66] Barbulescu R, Gadury P, Kleinjung T. The tower number field sieve[C]//ASIACRYPT 2015. Berlin:Springer, 2015: 31-55.

[67] Guillevic A. Computing Individual Discrete Logarithms Faster in GF(p^n) with the NFS-DL Algorithm[C]//ASIACRYPT 2015. Berlin:Springer, 2015: 149-173.

[68] Guillevic A. Faster individual discrete logarithms in finite fields of composite extension degree[J]. Mathematics of Computation, 2018, 88(2019): 1273-1301.

[69] Zhu Y Q, Wen J J, Zhuang J C, et al. Refined analysis to the extended tower number field sieve[J]. Theoretical Computer Science, 2020, 814: 49-68.

[70] Liu L W, Xu M Z. Improvements to the descent step in the number field sieve for discrete logarithms[C]//International Conference on Computer, Information and Telecommunication Systems (CITS). Piscataway: IEEE, 2020.

[71] Boudot F, Gaudry P, Guillevic A, et al. Comparing the difficulty of factorization and discrete logarithm: A 240-Digit Experiment[C]//Crypto 2020. Springer, 2020: 62-91.

[72] Fried J, Gaudry P, Heninger N, et al. A kilobit hidden SNFS discrete logarithm computation[C]//Eurocrypt 2017. Belin: Springer, 2017: 202-231.

[73] Coppersmith D. Fast evaluation of logarithms in fields of characteristic two[J]. IEEE Transactions on Information Theory, 1984, 30(4): 587-593.

[74] Adleman L M. The function field sieve[C]//Ants. Berlin: Springer, 1994: 108-121.

[75] Adleman L M, Huang M D. Function field sieve method for discrete logarithms over finite fields[J]. Information and Computation, 1999, 151: 5-16.

[76] Joux A, Lercier R. The function field sieve in the medium prime case[C]//Eurocrypt. Berlin: Springer, 2006:254-270.

[77] Joux A. A new index calculus algorithm with complexity L(1/4 + o(1)) in small characteristic[C]//SAC. Berlin: Springer, 2013: 355-379.

[78] Cheng Q, Wan D Q, Zhuang J C. Traps to the BGJT-algorithm for discrete logarithms[J]. LMS Journal of Computation and Mathematics, 2014, 17: 218-229.

[79] Zhu Y Q, Zhuang J C, Lv C, et al. Classifying and generating exact coset representatives of $PGL_2(F_q)$ in $PGL_2(F_{q^2})$[J]. Finite Fields and their Applications, 2016, 42: 118-127.

[80] Xiao D Y, Zhuang J C, Cheng Q. Factor base discrete logarithms in Kummer extensions[J]. Finite Fields and their Applications, 2018, 53:205-225.

[81] Granger R, Kleinjung T, Lenstra A, et al. Computation of a 30750-bit binary field discrete logarithm[J]. Mathematics of computation, 2021, 90(332): 2997-3022.

[82] 张方国, 陈晓峰, 王育民. 椭圆曲线离散对数的攻击现状[J]. 西安电子科技大学学报(自然科学版), 2002, 29(3): 398-403.

[83] 田松, 李宝, 王鲲鹏. 椭圆曲线离散对数问题的研究进展[J]. 密码学报, 2015, 2:177-188.

[84] 李俊全,刘木兰. 椭圆曲线素阶群上的离散对数问题[J]. 系统科学与数学, 2004, 24(4):443-450.

[85] Gallant R, Lambert R, Vanstone S. Improving the parallelized Pollard lambda search on binary anomalous curves[J]. Mathematics of Computation, 2000, 69(232): 1699-1705.

[86] Wiener M, Zuccherato R. Faster attacks on elliptic curve cryptosystems[C]//SAC 1998. Berlin:Springer, 1998: 190-200.

[87] Galbraith S, Ruprai R. Using equivalence classes to accelerate solving the discrete logarithm problem in a short interval[C]//PKC. Berlin: Springer, 2010: 368-383.

[88] Zhu Y Q, Zhuang J C, Yi H R, et al. A variant of the Galbraith-Ruprai algorithm for discrete logarithms with improved complexity[J]. Designs, Codes and Cryptography, 2019, 87: 971-986.

[89] Zhang F, Wang P. Speeding up elliptic curve discrete logarithm computations with point halving[J]. Designs, Codes and Cryptography, 2013, 67(2): 197-208.

[90] Wu H X, Zhang J C. Improving the Gaudry-Schost algorithm for multidimensional discrete logarithms[J]. Design, Codes

and Cryptography,2021. doi:10.1007/s10623-021-00966-5.

[91] Menezes A, Okamoto T, Vanstone S. Reducing elliptic curve logarithms to logarithms in a finite field[J]. IEEE Transactions on Information Theory, 1993, 39(5): 1639-1646.

[92] Frey G, Rück H. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves[J]. Mathematics of Computation, 1994, 62(206): 865-874.

[93] 白国强, 肖国镇, 马润年. 化离散对数问题为特殊的椭圆曲线离散对数问题[J]. 西安电子科技大学学报(自然科学版), 2001, 28(2): 254-257.

[94] 翁江, 扈瑜龙, 马传贵. F_{q^k}上阶为 q^k-1 的椭圆曲线离散对数问题研究[J]. 信息工程大学学报, 2018, 19(1):74-79.

[95] Smart N P. The discrete logarithm problem on elliptic curves of trace one[J]. Journal of Cryptology, 1999, 12(3): 193-196.

[96] Satoh T, Araki K. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves[J]. Commentarii Mathematici Universitatis Sancti Pauli, 1998, 47(1): 81-92.

[97] Semaev I. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p[J]. Mathematics of Computation, 1998, 67(221): 353-356.

[98] 朱玉清, 庄金成, 于伟, 等. 特征 p 椭圆曲线上 p 群的离散对数问题[J]. 密码学报, 2018, 5(4): 368-375.

[99] 祝跃飞, 裴定一. 求异常椭圆曲线上的 DLP 的一个算法[J]. 中国科学, 2001, 31(4): 332-336.

[100] Adleman L, DeMarrais J, Huang M. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields[C]//Ants. Berlin:Springer, 1994: 28-40.

[101] Gaudry P, Thome E, Theriault N, et al. A double large prime variation for small genus hyperelliptic index calculus[J]. Mathematics of Computation, 2007, 76(257): 475-492.

[102] Diem C. On the discrete logarithm problem in class groups of curves[J]. Mathematics of Computation, 2011, 80(273): 443-475.

[103] Frey G, Gangl H. How to disguise an elliptic curve (Weil descent)[R]. Talk at ECC'98, 1998.

[104] Galbraith S, Smart N. A cryptographic application of Weil descent[C]//IMA International Conference on Cryptography and Coding. Berlin:Springer, 1999: 191-200.

[105] Gaudry P, Hess F, Smart N. Constructive and destructive facets of Weil descent on elliptic curves[J]. Journal of Cryptology, 2002, 15(1): 19-46.

[106] Diem C. The GHS-attack in odd characteristic[J]. Journal of the Ramanujan Mathematical Society, 2003, 18(1): 1-32.

[107] Semaev I. Summation polynomials and the discrete logarithm problem on elliptic curves[J]. Cryptology ePrint Archive: Report, 2004/031, 2004.

[108] Gaudry P. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem[J]. Journal of Symbolic Computation, 2009, 44(12): 1690-1702.

[109] Diem C. On the discrete logarithm problem in elliptic curves[J]. Compositio Mathematica, 2011, 147: 75-104.

[110] Huang M, Kosters M, Yeo S. Last fall degree, HFE, and Weil descent attacks on ECDLP[C]//Crypto 2015. Berlin: Springer, 2015: 581-600.

[111] Huang M, Kosters M, Yang Y, et al. On the last fall degree of zero-dimensional weil descent systems[J]. Journal of Symbolic Computation, 2018, 87:207-226.

[112] Faugère J, Gaudry P, Huot L, et al. Using symmetries in the index calculus for elliptic curves discrete logarithm[J]. Journal of Cryptology, 2014, 27(4): 595-635.

[113] Faugère J, Huot L, Joux A, et al. Symmetrized summation polynomials: Using small order torsion points to speed up elliptic curve index calculus[C]//Eurocrypt 2014. Berlin:Springer, 2014: 40-57.

[114] Semaev I. New algorithm for the discrete logarithm problem on elliptic curves[R]. Cryptology ePrint Archive, Report 2015/310, 2015.

[115] Galbraith S, Granger R, Merz S, et al. On index calculus algorithms for subfield curves[R]. Cryptology ePrint Archive, Report 2020/1315, 2020.

【责任编辑: 陈 钢】