软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*,2013,24(Suppl.(2)):216−221

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

# 对区间上利用等价类解离散对数算法的改进*

张国良[1], 胡 志[2], 徐茂智[1]

[1](北京大学 数学科学学院 数学及其应用教育部重点实验室,北京 100871)

[2](北京大学 北京国际数学研究中心,北京 100871)

通讯作者: 徐茂智, E-mail: mzxu@math.pku.edu.cn

**摘 要**: Pollard kangaroo 算法是解决区间 $N$ 上离散对数问题很有效的方法,在平均意义下需要进行 $2\sqrt{N}$ 次群操作.而 Galbraith 和 Ruprai 对容易进行求逆运算的群,利用等价类的方法,将平均意义下需要的群操作次数降低到了 $1.36\sqrt{N}$ .在 Galbraith 和 Ruprai 的基础上,对算法进行了优化,调整了家袋鼠和野袋鼠的活动区间,将区间分别变为了原来的 0.8581 倍,从而将平均意义下需要的群操作次数降低到了 $1.338\sqrt{N}$ .

**关键词**: 离散对数问题;椭圆曲线;袋鼠算法;逆映射;等价类

中文引用格式: 张国良,胡志,徐茂智.对区间上利用等价类解离散对数算法的改进.软件学报,2013,24(Suppl.(2)):216−221. http://www.jos.org.cn/1000-9825/13039.htm

英文引用格式: Zhang GL, Hu Z, Xu MZ. Improvements on the discrete logarithm algorithm with equivalence classes. Ruan Jian Xue Bao/Journal of Software, 2013,24(Suppl.(2)):216−221 (in Chinese). http://www.jos.org.cn/1000-9825/13039.htm

## Improvements on the Discrete Logarithm Algorithm with Equivalence Classes

ZHANG Guo-Liang[1], HU Zhi[2], XU Mao-Zhi[1]

[1](LMAM, School of Mathematical Sciences, Peking University, Beijing 100871, China)

[2](Beijing International Center for Mathematical Research, Peking University, Beijing 100871, China)

Corresponding author: XU Mao-Zhi, E-mail: mzxu@math.pku.edu.cn

**Abstract**: The pollard kangaroo method is a very effective way to solve the discrete logarithm problem in an interval of size $N$, which needs approximately $2\sqrt{N}$ group operations under heuristic average case. For those fast inversion groups, Galbraith and Ruprai use equivalence classes method to lower the times of group operations which are needed under heuristic average case to approximately $1.36\sqrt{N}$ .Based on Galbraith and Ruprai, this paper optimizes the method and adjusts the active interval of the tame kangaroos and wild kangaroos, in a way of changing each of their intervals to approximately 0.8581 times the original one, so that the group operations under heuristic average case is lowered to approximately $1.338\sqrt{N}$ .

**Key words**: discrete logarithm problem; elliptic curves; pollard kangaroo method; inverse map; equivalence class

## 1 简 介

设 $G$ 为阶是 $r$ 的有限 Abel 群,$g,h\in G$.若 $h=g^n$ 并已知 $n\in(0,N)$对某个正整数 $N\leqslant r$,求解 $n$ 即为计算区间上的离散对数问题.离散对数问题是现代密码学中的一个非常重要的问题,很多加密体制和协议都是依赖于假定的离散对数问题的计算难度,例如 ElGmal 系统[1],数字签名算法(DSA)[2]等.Pollard[3]最早提出用 kangaroo 算法来计算一般有限 Abel 群上的离散对数问题,而利用 distinguished point,van Oorschot 和 Wiener[4]将 Pollard kangaroo 算法在平均意义下需要的群操作次数降为 $2\sqrt{N}$ ,且只需较低的存储量.基于 Gaudry 和 Harley[5]之前的工作,Gaudry 和 Schost[6]利用生日攻击的分析方法找到了一种不同的计算离散对数的方法,虽然他们的方法没

* 基金项目: 国家自然科学基金(61272499,10990011); 信息保障技术重点实验室(KJ-11-02)
收稿时间: 2013-07-17; 定稿时间: 2013-10-16

有 van Oorschot 和 Wiener 的快,但更易于并行计算,而且重要的是在算法开始前,不需要知道计算者的数量,平均意义下的群操作次数为 $2.08\sqrt{N}$ .Galbraith 和 Ruprai[7]则是利用 Gaudry 和 Schost 方法,对于容易进行求逆运算的群,利用等价类的方法,对袋鼠的活动区间重新定义,使得平均意义下的群操作次数降为 $1.36\sqrt{N}$ .

## 2 Galbraith 和 Ruprai 的算法

对于一般的区间离散对数问题,可将其转化为关于 0 对称区间的离散对数问题.记 $g$ 和 $h$ 与之前符号相同,那么可以令 $h$ 除以 $g^{\frac{N}{2}}$,仍记为 $h$,则离散对数问题就变为了 $h=g^n$,其中 $-N/2\leqslant n\leqslant N/2$,这样的记法主要是为了方便利用逆映射来加速运算.

Galbraith 和 Ruprai 的算法是基于 Gaudry 和 Schost 的工作,利用生日攻击的分析方法和等价类进行的改进,下面进行简单介绍.

### 2.1 分析方法与技巧

**定理 1(Selivanov)**. 当在一个大小为 $R$ 的集合里有放回的均匀地随机选取元素,$R\in N$,交替记录在两个不同的表里,那么在发现两表之间出现一个元素重合之前,选取的期望次数为 $\sqrt{\pi R}+O(1)$.

这是生日攻击分析方法中最核心的部分,也是 Galbraith 和 Ruprai 的算法中最主要的分析方法.

至于等价类,在此处特指对于易于计算逆映射的群,利用逆映射得到的等价类,即将 $\{a,-a\}$ 看作一个等价类,当得知 $a$ 值时,忽略 $-a$ 的计算用时,例如对于椭圆曲线 $E:y^2=x^3+Ax+B$,对于任意点 $P=(x,y)\in E$,可以很容易地计算得到 $-P=(x.-y)$,从而在计算的时候,经过一次点的运算就可以得到两个点的结果.

### 2.2 Galbraith和Ruprai的算法定义

Galbraith 和 Ruprai 的算法与原始的 kangaroo 算法相同,分为两种不同的探测方法,将它们分别记为家袋鼠和野袋鼠,家袋鼠就是指形为 $g^a$ 元素组成的集合,而野袋鼠是指形为 $hg^a=g^{n+a}$ 的元素组成的集合.由于元素的底数都是 $g$,所以只研究指数部分.由于目标离散对数群上易于进行求逆运算,故考虑使用等价类的方法,将元素成对进行考虑,从而重新定义算法的探测区间,新的区间定义如下,家袋鼠的指数在算法中为

$$T=\left\{\{a,-a\}:a\in\left[-\frac{N}{2},\frac{N}{2}\right]\right\},$$

而野袋鼠的指数为

$$W=\left\{\{n+a,-(n+a)\}:a\in\left[-\frac{N}{4},\frac{N}{4}\right]\right\},$$

其中,

$$[N_1,N_2]=\{a\in Z:N_1\leqslant a\leqslant N_2\}.$$

以上就是 Galbraith 和 Ruprai 算法的定义,利用伪随机游走,在区间上进行随机选取,然后通过寻找碰撞来解决离散对数问题.

### 2.3 Galbraith和Ruprai的算法分析

利用等价类定义出的 $T$ 和 $W$ 分为正负两部分,为了分析方便,利用两者的对称关系,只考虑正的区间部分即可.在取正的过程中,因为 $W$ 在某些时候会出现重叠部分,这样就会使碰撞的概率加大,这样不均匀的分布会影响算法的实际效果,故重叠的部分在分析时也应考虑为两次,那么正的区间定义为

$$\tilde{T}=\left[0,\frac{N}{2}\right],\tilde{W}=\left\{|n|+a:a\in\left[-|n|,\frac{N}{4}\right]\right\}\cup\left\{-(|n|+a):a\in\left[-\frac{N}{4},-|n|\right]\right\}=\left[0,|n|+\frac{N}{4}\right]+\left[0,\frac{N}{4}-|n|\right].$$

**定理 2**[7]. 令 $R\in N$ 和 $0\leqslant A\leqslant R/2$,假设有两种不同颜色的无限数量的球,分别记为红色和蓝色,此外有 $R$ 个缸.假定交替地从每种颜色的球中选取一个,并将其放入随机的缸中.红色球进入缸中的概率是均匀并且独立和随机的,蓝色球进入缸中的概率也是独立和随机的,但并不均匀,蓝色球以 $2/R$ 的概率进入 $1\leqslant u\leqslant A$ 号缸,以

$1/R$ 的概率进入 $A<u\leqslant R-A$,以 0 的概率进入 $R-A<u\leqslant R$,那么在一个缸里有两种不同颜色的球之前,操作的次数期望为 $\sqrt{\pi R}+O\left(R^{\frac{1}{4}}\right)$.

**定理 3**[7]. 若 $T$ 和 $W$ 以及所有相关的变量的定义如 Galbraith 和 Ruprai 算法中所示,那么在找到一个家袋鼠和野袋鼠碰撞前,群操作次数的期望为

$$\left(\frac{5\sqrt{2}}{4}-1\right)\sqrt{\pi N}+O\left(N^{\frac{1}{4}}\right)\approx 1.36\sqrt{N}\ .$$

这是 Galbraith 和 Ruprai 得到的结论,将算法中群操作次数期望减少到了 $1.36\sqrt{N}$.在接下来的章节里将介绍改进的算法.

## 3 对 Galbraith 和 Ruprai 算法的改进

通过对 Galbraith 和 Ruprai 算法的分析,不难看出该算法相对于之前算法的不同在于利用等价类后,有部分探测区域会有重叠的情况出现,而这些重叠并不是无意义的,在考虑碰撞情况的时候,起到了增强的效果.而根据算法的定义,重叠的区域主要集中在 0 点附近,也就是说在 0 点附近取的值多,从而以较大的概率出现碰撞.

那么如果将探测区域尽力压缩到 0 点附近,出现碰撞的可能性会加大,这样就会减少在出现碰撞前所需要的操作次数.但是如果探测区间选的过小,可能会出现家袋鼠和野袋鼠区间无法相交,导致算法失败,故不能将探测区间选的过小.综合这两个因素,对探测区间进行选择,找到更好的结果.

### 3.1 改进方法与分析

类似于文献[8]中对区间考虑的方法,我们对原始的 Galbraith 和 Ruprai 算法,考虑对其探测区间进行等比例缩小的方法,也就是说重新定义家袋鼠的指数在算法中为 $T=\left\{\{a,-a\}:a\in\left[-\frac{\alpha N}{2},\frac{\alpha N}{2}\right]\right\}$,而野袋鼠的指数为 $W=\left\{\{n+a,-(n+a)\}:a\in\left[-\frac{\alpha N}{4},\frac{\alpha N}{4}\right]\right\}$,其中 $0<\alpha\leqslant 1$,其他部分与原有算法保持不变.根据这个新定义的 $T$ 和 $W$,可以得到 $\tilde{T}=\left[0,\frac{\alpha N}{2}\right]$.

当 $|n|<\frac{\alpha N}{4}$ 时,$\tilde{W}=\left\{|n|+a:a\in\left[-|n|,\frac{\alpha N}{4}\right]\right\}\bigcup\left\{-(|n|+a):a\in\left[-\frac{\alpha N}{4},-|n|\right]\right\}=\left[0,|n|+\frac{\alpha N}{4}\right]+\left[0,\frac{\alpha N}{4}-|n|\right]$.

当 $|n|\geqslant\frac{\alpha N}{4}$ 时,$\tilde{W}=\left\{|n|+a:a\in\left[-\frac{\alpha N}{4},\frac{\alpha N}{4}\right]\right\}$.

首先,考虑算法是否能得到解的问题,也就是说 $\tilde{T}$ 和 $\tilde{W}$ 是否能够一直存在相交的部分,如果在某种情况下不存在相交的部分,那么算法无论进行多少次计算,都无法得到结果.

由于 $\tilde{W}$ 是关于 $n$ 变化的,并且可以看出,当 $|n|<\frac{\alpha N}{4}$ 时,$\tilde{T}$ 必定与 $\tilde{W}$ 有交集,那么只考虑 $|n|\geqslant\frac{\alpha N}{4}$ 的情况即可.因为 $0\leqslant|n|\leqslant\frac{N}{2}$,此时若使得 $\tilde{T}$ 和 $\tilde{W}$ 一直存在交集,应有 $\frac{N}{2}-\frac{\alpha N}{4}\leqslant\frac{\alpha N}{2}\leqslant\frac{N}{2}$,得到 $\frac{2}{3}\leqslant\alpha\leqslant 1$,这样就能保证算法一定能得到解.

下面,在 $\frac{2}{3}\leqslant\alpha\leqslant 1$ 的前提下,计算在得到一个家袋鼠野袋鼠碰撞之前,平均意义下的群操作次数,再进一步使用分析方法,求出使得群操作次数达到最小的 $\alpha$.

**定理 4**. 若重新定义家袋鼠区间 $T=\left\{\{a,-a\}:a\in\left[-0.8581\frac{N}{2},0.8581\frac{N}{2}\right]\right\}$ 和野袋鼠区间

$W=\left\{\{n+a,-(n+a)\}:a\in\left[-0.8581\frac{N}{4},0.8581\frac{N}{4}\right]\right\}$,而其他所有相关变量的定义如 Galbraith 和 Ruprai 算法中所示,那么在找到一个家袋鼠和野袋鼠碰撞前,群操作次数的期望为 $1.338\sqrt{N}$.

证明:为了方便分析和计算,对于 $h=g^n$,其中 $-\frac{N}{2}\leqslant n\leqslant\frac{N}{2}$,记 $|n|=xN$,其中 $0\leqslant x\leqslant\frac{1}{2}$.

当 $0\leqslant x<\frac{\alpha}{4}$ 时,$\tilde{W}\subseteq\tilde{T}$,在 $\tilde{W}\cap\tilde{T}$ 取值进行探测的时候,在 $\tilde{T}$ 中是均匀随机选取,而在 $\tilde{W}$ 中是不均匀的.而当 $\frac{\alpha}{4}\leqslant x\leqslant\frac{1}{2}$ 时,在 $\tilde{W}$ 和 $\tilde{T}$ 上的选取都是均匀的.从而将情况分成这两种,第 1 种利用生日攻击的方法来分析,第 2 种利用均匀分布的方法进行分析.

当 $0\leqslant x<\frac{\alpha}{4}$ 时,根据 $\tilde{T}=\left[0,\frac{\alpha N}{2}\right]$ 是均匀的,$\tilde{W}=\left[0,|n|+\frac{\alpha N}{4}\right]+\left[0,\frac{\alpha N}{4}-|n|\right]$ 可以看出,重叠的部分为 $\left[0,\frac{\alpha N}{4}-|n|\right]$,取值一次的部分为 $\left[\frac{\alpha N}{4}-|n|,|n|+\frac{\alpha N}{4}\right]$,在 $\left[\frac{\alpha N}{4}+|n|,\frac{\alpha N}{2}\right]$ 处取不到值,利用定理 2,将定理中的 $R$ 换成 $\frac{\alpha N}{2}$,可以得到在得到碰撞之前,需要的群操作次数期望为 $\sqrt{\frac{\pi\alpha N}{2}}+O\left(N^{\frac{1}{4}}\right)$.

当 $\frac{\alpha}{4}\leqslant x\leqslant\frac{1}{2}$ 时,在 $\tilde{W}$ 和 $\tilde{T}$ 上的选取都是均匀的,只需要考虑两者的相交区域即可,不难看出 $|\tilde{W}\cap\tilde{T}|=\frac{3\alpha N}{4}-xN$,从而根据定理 1,在 $\tilde{W}\cap\tilde{T}$ 上面选点,在得到一个碰撞之前需要的群操作次数期望为 $\sqrt{\pi|\tilde{W}\cap\tilde{T}|}$ .但若在 $\tilde{W}$ 和 $\tilde{T}$ 上随机选点,而 $|\tilde{W}|=|\tilde{T}|=\frac{\alpha N}{2}$,这种情况下在得到一个碰撞之前,需要的群操作次数期望为

$$\frac{|\tilde{T}|}{|\tilde{T}\cap\tilde{W}|}\sqrt{\pi|\tilde{W}\cap\tilde{T}|}=\frac{\frac{\alpha N}{2}}{\frac{3\alpha N}{4}-xN}\sqrt{\pi\left(\frac{3\alpha N}{4}-xN\right)}=\frac{\alpha}{2}\sqrt{\frac{\pi N}{\left(\frac{3\alpha}{4}-x\right)}}.$$

接下来对这两种情况中期望的群操作次数进行估计.第 1 种情况下需要的群操作次数期望是一个常数,而第 2 种情况下是一个关于 $x$ 的变量,利用积分的方法进行估计,所需要的群操作次数期望为

$$2\int_0^{\frac{\alpha}{4}}\sqrt{\frac{\pi\alpha N}{2}}\mathrm{d}x+2\int_{\frac{\alpha}{4}}^{\frac{1}{2}}\frac{\alpha}{2}\sqrt{\frac{\pi N}{\left(\frac{3\alpha}{4}-x\right)}}\mathrm{d}x.$$

通过对积分的计算以及化简,将得到的结果记为 $f$,有如下结果:

$$f=\frac{5\alpha}{4}\sqrt{2\pi\alpha N}-\alpha\sqrt{\pi N(3\alpha-2)}.$$

如上所述,$f$ 为一般情况下遇到碰撞前所需要的群操作次数期望,则对 $\alpha$ 进行分析,使上式达到最小,其中要求 $\frac{2}{3}\leqslant\alpha\leqslant1$.对 $f$ 求导得到 $\frac{\mathrm{d}f}{\mathrm{d}\alpha}=\frac{5}{4}\sqrt{2\pi\alpha N}\times\frac{3}{2}-\sqrt{\pi N(3\alpha-2)}-\frac{\frac{3\alpha}{2}\sqrt{\pi N}}{\sqrt{3\alpha-2}}$ 令导数等于 0,寻找极值点,整理后得到等式 $15\sqrt{2\alpha(3\alpha-2)}=4(9\alpha-4)$,解得 $\alpha=\frac{-126\pm\sqrt{29700}}{2\times27}=\frac{-21\pm5\sqrt{33}}{9}$.

由于 $\frac{2}{3}\leqslant\alpha\leqslant1$,所以上式中 ± 号只能取正号,此时 $\alpha=0.8581$ 为此区间上唯一极值点,利用 $\alpha$ 附近的值代入 $f$ 的导数,根据连续函数的性质,可以知道 $f$ 的导数在 $\alpha$ 左侧小于 0,$\alpha$ 右侧大于 0,也就是说 $\alpha$ 为该区间上 $f$ 的最小值所对应的值,将 $\alpha$ 的值代入 $f$,即可得到 $f_{\min}=1.338\sqrt{N}$.

### 3.2 算法描述

对于 Galbraith 和 Ruprai 算法改进了家袋鼠和野袋鼠的探测区间,这就涉及到了探测过程中的伪随机游走,以及越界判断的改变,下面将算法的全部过程重新给出.

虽然计算离散对数问题的很多方法都用到伪随机游走来寻找碰撞,但是区间上离散对数问题的伪随机游走与其他算法是不同的.为了方便描述,以椭圆曲线作为例子,考虑 $Q=[n]P$,并已知 $-\frac{N}{2}\leqslant n\leqslant\frac{N}{2}$,求解这个区间离散对数问题.

记每一次袋鼠跳的结果为 $R_i$,虽然同样形式为 $R_{i+1}=R_i+\left[u_{S(R_i)}\right]P$,其中 $S$ 是将群的不同子集映射到整数 $\{0,1,2,\ldots,n_s\}$ 上的函数,但是 $u_j\,(0\leqslant j\leqslant n_s)$ 是相对较小的随机数,以保证在达到 distinguished point 之前不会跳出界限.记 $\theta$ 为达到 distinguished point 的概率,如果取 $-m\leqslant u_j\leqslant m$,那么根据下面的定理 4,应该选择 $m\sqrt{\frac{2}{3\pi\theta}}\approx\sqrt{N}$,这样仅仅有长度为 $\sqrt{N}$ 的区间不可以作为起点.

**定理 5**[9]. 记 $y_0=0,y_1,\ldots,y_k$ 是从 0 开始的对称随机游走,每一步的步长随机选取于[−1,1],那么最大的位移值期望为 $E\left(\max\{|y_i|:0\leqslant i\leqslant k\}\right)=\sqrt{\frac{2k}{3\pi}}+O(1)$.

根据 $\theta$ 的定义可知,遇到 distinguished point 之前需要的步数期望为 $\frac{1}{\theta}$,即为上式的 $k=\frac{1}{\theta}$,故该算法中遇到 distinguished point 之前需要的位移长为 $m\sqrt{\frac{2}{3\pi\theta}}$.

由于 $u_j$ 都是提前随机选好的,可以将 $\left[u_j\right]P$ 提前进行预计算,以加快算法运行.除了要求步长比较小以外,为了不容易跳出规定的界限,也要限定袋鼠跳跃的起点,比如要求家袋鼠的起点为 $[a]P$,其中

$$a\in\left[-0.8581\frac{N}{2}+m\sqrt{\frac{2}{3\pi\theta}},0.8581\frac{N}{2}-m\sqrt{\frac{2}{3\pi\theta}}\right],$$

野袋鼠的起点为 $Q+[a]P$,其中,

$$a\in\left[-0.8581\frac{N}{4}+m\sqrt{\frac{2}{3\pi\theta}},0.8581\frac{N}{4}-m\sqrt{\frac{2}{3\pi\theta}}\right].$$

由于不是每条路径上都肯定能跳到 distinguished point,所以需要设定一个跳跃次数的限制,一旦达到了,就重新选择起点,而不是一直计算下去,在这里面选择次数限制为 $\frac{20}{\theta}$.

**算法 1**. 家袋鼠计算过程.

输入:区间长度 $N$,点 $P$,点 $Q$.

输出:元素$(R,a_T)$.

1. 随机选取 $a_1\in\left[-0.8581\frac{N}{2}+m\sqrt{\frac{2}{3\pi\theta}},0.8581\frac{N}{2}-m\sqrt{\frac{2}{3\pi\theta}}\right]$.
2. 计算 $R_1=[a_1]P$, $number=0$.
3. 重复以下(a)和(b),直到 $R_i$ 是 distinguished point 或者 $number>\frac{20}{\theta}$ 或者 $a_i\notin\left[-0.8581\frac{N}{2},0.8581\frac{N}{2}\right]$时,
   a) $(R_{i+1},a_{i+1})=walk(R_i,a_i)$
   b) *number*增加 1

4. 如果 $R_i$ 是 distinguished point,将元素 $(R_i,a_i)$ 与列表中进行比较.

5. 如果没有得到中止的指令,返回到步骤 1,继续计算.

野袋鼠算法改变相应的区间、起始点 $R_1=[a_1]P+Q$ 即可,将两个算法得到的值返回列表寻找碰撞,与以往算法不同的是,此时要将 $\{R,-R\}$ 同时进行比较.如果发生碰撞则解决离散对数问题;如果没有发生碰撞,则存储数据后继续进行探测.

## 4 总 结

通过对 Galbraith 和 Ruprai 的算法中家袋鼠和野袋鼠的探测区间进行改进,使得重叠部分的权重加大,以提高算法效率,将得到一次碰撞前,平均意义下的群操作次数期望从 $1.361\sqrt{N}$ 减少到 $1.338\sqrt{N}$ .

**References**:


[1] ElGamal E. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory, 1985,31(4):469–472.

[2] FIPS 186-2. Digital signature standard. Federal Information Processing Standards Publication 186-2, 2000.

[3] Pollard JM. Monte Carlo methods for index computation (mod *p*). Mathematicsof Computation, 1978,32:918–924.

[4] van Oorschot PC, Wiener MJ. On Diffie-Hellman key agreement with short exponents. In: Maurer U, ed. In: Proc. of the EUROCRYPT 1996. LNCS, Springer-Verlag, 1996. 332–343.

[5] Gaudry P, Harley R. Counting points on hyperelliptic curves over finite fields. In: Bosma W, ed. Proc. of the Algorithm Number Theory Symp. ANTSIV. Springer-Verlag, 2000. 313–332.

[6] Gaudry P, Schost E. A low-memory parallel version of Matsuo, Chao and Tsu-jii's algorithm. In: Buell DA, ed. Proc. of the Algorithm Number Theory Symp.—ANTS VI. LNCS, Springer-Verlag, 2004. 208–222.

[7] Galbraith SD, Ruprai RS. Using equivalence classes to accelerate solving the discrete logarithm problem in a short interval. In: Nguyen P, Pointcheval D, eds. Public Key Cryptography—PKC 2010. Springer-Verlag, 2010. 368–383.

[8] Galbraith SD, Pollard JM, Ruprai RS. Computing discrete logarithms in an interval. Mathematics of Computation, 2013,82: 1181–1195.

[9] Coffman EG, Flajolet P, Flatto L, Hofri M. The maximum of a random walk and its application to rectangle packing. Probability in the Engineering and Informational Sciences, 1998,12(3):373–386.



**张国良**(1988－),天津人,男,博士生,主要研究领域为密码学,信息安全理论.
E-mail: guoliang_tj@126.com



**徐茂智**(1962－),男,博士,教授,博士生导师,主要研究领域为代数学,密码学.
E-mail: mzxu@pku.edu.cn



**胡志**(1985－),男,博士,主要研究领域为密码学,信息安全理论.
E-mail: huzhi@math.pku.edu.cn