离散对数问题攻击算法的改进

汤鹏志,何 涛,李 彪
(华东交通大学 基础科学学院,江西 南昌 330013)

摘 要:在求解离散对数问题上有袋鼠攻击、生日攻击、小步-大步攻击、指数积分攻击等多种方法,而小步-大步攻击算法是比较通用且高效的。为了提高攻击算法的速度,改善算法的效率,提出的改进算法牺牲了适当的存储空间,但在运算之前通过奇偶判断筛选过程减少了判断的次数甚至有数量级的减少。性能分析表明,改进的算法在性能上优于原算法。并且预处理过程中产生的数据可以重复利用来求解同一群下不同生成元的离散对数问题,这又进一步减少了算法的运算复杂度。

关键词:离散对数;小步-大步攻击算法;奇偶判断
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2013)05-0127-04
doi:10.3969/j.issn.1673-629X.2013.05.033

Improved Attack Algorithm for Discrete Logarithm Problem

TANG Peng-zhi,HE Tao,LI Biao
(School of Basic Science,East China Jiaotong University,Nanchang 330013,China)

Abstract:There are kangaroo attack,birthday attack,baby-step-giant-step attack,exponential integral attack and other methods in solving the discrete logarithm problem. The baby-step-giant-step attack algorithm is more versatile and efficient. In order to improve the speed of the attack algorithm and the efficiency of the algorithm,the algorithm proposed is improved at the expense of the appropriate storage space. By the parity operator before the judge selection process reduce the number of judgment,even the reduction of the magnitude. The performance analysis shows that the improved algorithm outperforms the original algorithm. And the data generated in the pretreatment process can be reused to solve the problem of the generator under the same group of discrete logarithm. This further reduces the computational complexity of the algorithm.

Key words:discrete logarithm;baby-step-giant-step attack algorithm;parity judgment

0 引 言

离散对数公钥加密算法是目前最为热门的加密算法,其安全性远远高于 RSA 算法,Diffie-Hellman 密钥协议、ElGamal 密码体制及其相关变种的签名方案都是建立在离散对数问题之上。针对离散对数问题的攻击方法,已知的指数积分攻击[1]、小步-大步攻击[2]、袋鼠攻击[3]、生日攻击[3]等攻击算法,不同的攻击算法针对基于不同群下的离散对数问题效率不一,Pollard-Hellman[4]算法针对群的阶只有小素因子时攻击特别有效,而 index-calculus[4]算法是亚指数攻击算法,只对特定的群有效。传统的小步-大步攻击算法由于构建了链表,执行过程中的查表操作大大降低了算法的效率,增加了算法的执行时间。

同时由于基于离散对数问题的各种签名方案[5~7]的提出,如何有效地利用离散对数构造安全有效的方案也是面临的难题,所以从离散对数问题的攻击方法入手,可以更好地通过离散对数问题提出更有效的方案。文中结合文献[8]提出的奇偶判断思想,提出了一种新的攻击离散对数的方法,与传统算法比较该算法提高了执行效率并降低了时间复杂度。

1 预备知识

给定一个元素 y,且已知存在一个整数 x,对一个固定的基 b,有 $y=b^x$,如何求解 x,就是一个离散对数问题。

定义 1:给定一个素数 p,Z_p^* 的一个生成元 α 及一个元素 $\beta \in Z_p^*$,寻找整数 $x(0 \leqslant x \leqslant p-2)$,使得 $\alpha^x \equiv \beta \bmod p$。

上述给出的是离散对数问题的定义,直观上看该

收稿日期:2012-08-02;**修回日期**:2012-11-05
基金项目:国家自然科学基金资助项目(11061014);江西省教育青年科学基金项目(GJJ11675);江西省教育科研项目(GJJ11678)
作者简介:汤鹏志(1961-),男,江西九江人,硕士,教授,主要研究方向为信息系统及其安全;何 涛(1990-),男,江西丰城人,硕士研究生,主要研究方向为信息安全。

问题的困难性取决于问题的规模以及参数的选择,根据离散对数假设[4]可知在充分大的有限域中,对于所有的情形,不存在求解离散对数问题的有效算法。然而现实世界中事物是有界的,则一定存在多项式时间解法。通过规定适当的下界使得多项式时间解法所运行的时间是一个难以对付的大数,正因如此该问题的难解性构成了包括 Diffie-Hellman 密钥分配,ElGamal 公钥密码等在内的很多密码体制的安全性基础[9,10]。

定理 1:设 $G=\langle a\rangle$ 是循环群,则有:

(1)若 G 是无限循环群,则 G 只有两个生成元,即 a 和 a^{-1}。

(2)若 G 是 n 阶循环群,则 G 含有 $\varphi(n)$ 个生成元,对于任何小于等于 n 且与 n 互质的正整数 r,a^r 是 G 的生成元。

证明(1):显然 $\langle a^{-1}\rangle \subseteq G$,对于任何 $a^k \in G$,a^k 都可以表示成为 a^{-1} 的幂,则可以得到 $a^k=(a^{-1})-k$,从而得到 $G\subseteq\langle a^{-1}\rangle$,则 a^{-1} 是 G 的生成元。

假设 b 也是 G 的生成元,则 $G=\langle b\rangle$,由 $a\in G$ 可知存在整数 t,使得 $a=b^t$。又由 $b\in G=\langle a\rangle$ 知存在整数 m,使得 $b=a^m$,从而有 $a=b^t=(a^m)^t=a^{mt}$,由消去律得 $a^{mt-1}=e$,因为 G 是无限群,必有 $mt-1=0$,从而证明 $m=t=1$ 或者 $m=t=-1$,即 $b=a$ 或者 $b=a^{-1}$。

(2) 只要证明:对于任何正整数 $r(r\leqslant n)$,a^r 是 G 的生成元当且仅当 n 与 r 互质。

充分性:设 n 与 r 互质,且 $r\leqslant n$,那么存在整数 u,v 使得 $ur+nv=1$,根据拉格朗日定理的推论有 $a=a^{ur+vn}=(a^r)^u(a^n)^v=(a^r)^u$,则可以推出 $\forall a^k\in G,a^k=(a^r)uk\in\langle a^r\rangle$,即 $G\subseteq\langle a^r\rangle$,显然可知 $\langle a^r\rangle\subseteq G$,从而有 $G=\langle a^r\rangle$。

必要性:设 a^r 是 G 的生成元,则 $|a^r|=n$,令 r 和 n 的最大公约数为 d,则存在正整数 t 使得 $r=dt$,则有 $(a^r)^{\frac{n}{d}}=(a^{dt})^{\frac{n}{d}}=(a^n)^t=e$,根据群的性质可知 $|a^r|$ 是 n/d 的因子,即 n 整除 n/d,从而证明了 $d=1$。

命题 1 若 $b^{n/2}=1\bmod p$,则 $\log_a b$ 是偶数,否则是奇数。

证明:设 $x=\log_a b\bmod n$,则 $b=a^x\bmod p$。由 $(a^{n/2})^2=a^n=1\bmod p$,则 $a^{n/2}=\pm 1\bmod p$。因 a 的阶为 n,有 $a^{n/2}\neq 1\bmod p$,从而 $b^{n/2}=a^{x\cdot n/2}=(-1)^x\bmod p$,也即 $b^{n/2}=1\bmod p$ 时,$\log_a b$ 是偶数,否则是奇数。

2 小步-大步攻击算法及分析

算法 1

Step1 $s\leftarrow 1,u\leftarrow 1,L_1\leftarrow$ Null,$m\leftarrow\lceil n^{\frac{1}{2}}\rceil$

Step2 for $j\leftarrow 0$ to $m-1$

Step2.1 $s\leftarrow a^{jm}$

Step3 根据第二个坐标对有序对 (j,a^{mj}) 进行排序,得到链表 L_1

Step4 for $i\leftarrow 0$ to $m-1$

Step4.1 $u\leftarrow ba^{-i}$

Step5 根据第二个坐标对有序对 (i,ba^{-i}) 进行排序,得到链表 L_2

Step6 通过查找 L_1 和 L_2 两个链表中 (j,a^{mj}) 和 (i,ba^{-i}) 中第二个坐标相同的有序对

Step7 $\log_a b\leftarrow(mj-i)\bmod n$ 结束

以群乘法为基本运算单位来分析该算法的时间和空间复杂度。

在 Step1 中为了快速计算首先要预先计算 a^m 并缓存,利用平方乘算法来进行高次幂运算,此步的时间复杂度为 $O(\log m)$。

在 Step2 中空间复杂度为 $O(m)$,一共要计算 m 次,时间开销为 $O(m)$。

在 Step3 中要对生成的有序对进行排序,利用快速排序算法,算法的时间复杂度为 $O(m\log m)$,空间复杂度为 $O(m)$,同样 Step5 的时间复杂度和空间复杂度和本步相同。

在 Step4 中空间复杂度为 $O(m)$,一共要计算 m 次,并且由于增加了求逆的运算,求逆的算法时间复杂度为 $O(\log a)$,Step4.1 的开销为 $O(m)$。

在 Step6 中由于要查找两个生成的链表中第二坐标相同的有序对,需要对两链表逐一比较,最大的比较次数为 $O(n)$,平均比较次数为 $O(n/2)$。

算法成功停机的充要条件是 $b\in\langle a\rangle$,$\langle a\rangle$ 为由 a 生成的群。

必要性:成功停机说明算法 1 的 Step6 中的等式 $a^{mj}=y=ba^{-i}$ 成立,则 $b=a^{(mj+i)}$,由于 $1\leqslant i,j\leqslant m$,有 $0\leqslant mj+i$,又 a 是生成元,所有 $b\in\langle a\rangle$。

充分性:因为 $b\in\langle a\rangle$,$0\leqslant\log_a b\leqslant n-1$,$m=\lceil n^{\frac{1}{2}}\rceil$,所以 $0\leqslant\log_a b\leqslant n-1\leqslant m^2-1$。令 $1\leqslant i\leqslant m$ 且 $\log_a b=mj+i$,则可知 $1\leqslant i\leqslant m$。当 i,j 满足 $1\leqslant i,j\leqslant m$ 时,$\log_a b$ 可以写成 $\log_a b=mj+i$。a 是生成元,有 $b=a^{(mj+i)}$,即 $a^{mj}=ba^{-i}$,则算法 1 的 Step6 一定可以成功,所以算法 1 可以成功停机。

3 改进的算法

首先利用算法 1 的结束条件计算出满足条件的 (i,j) 对,把 (i,j) 对根据命题 1 的奇偶判断条件进行奇偶性分组,然后通过命题 1 的判断结果得到 $\log_a b$ 的奇偶性,再结合 $\log_a b$ 和 (i,j) 对的奇偶性进行快速求解离散对数问题。给出算法如下:

算法 2

Step1 预处理

Step1.1 for $i \leftarrow 1$ to m

Step1.1.1 for $j \leftarrow 1$ to m

Step1.1.2 if $(mj - i) \equiv 1 \bmod 2n$

Step1.1.3 $L_1 \leftarrow (i,j)$ L_1 存储奇数 (i,j) 对

Step1.1.4 else $L_2 \leftarrow (i,j)$ L_2 存储偶数 (i,j) 对

Step2 系统初始化

Step2.1 $s \leftarrow 1, u \leftarrow 1, L_1 \leftarrow \text{Null}, L_2 \leftarrow \text{Null}, L_3 \leftarrow \text{Null}, L_4 \leftarrow \text{Null}$

Step2.2 $m \leftarrow \lceil n^{\frac{1}{2}} \rceil$, m 转换成具有较小海明权重[11]的表示形式

Step3 判断奇偶性

Step3.1 for $j \leftarrow 1$ to m

Step3.1.1 $s \leftarrow s \times a$

Step3.1.2 $L_3(s)$

Step3.2 for $i \leftarrow 1$ to m

Step3.2.1 $u \leftarrow u \times a$

Step3.2.2 $L_4(s)$

Step3.3 if $b^{n/2} = 1 \bmod p$ then

Step3.3.1 for (i,j) in $L_2(i,j)$

Step3.3.2 if $(L_3(j))^m = b \cdot L_4(i)$，运用多精度平方乘算法[12]计算 $(L_3(j))^m$

Step3.3.2.1 $\text{Log}_a b \leftarrow (mj - i) \bmod n$ 结束

Step3.3.3 else go to Step3.3.1

Step3.4 else

Step3.4.1 for (i,j) in $L_1(i,j)$

Step3.4.2 if $(L_3(j))^m = b \cdot L_4(i)$，运用多精度平方乘算法计算 $(L_3(j))^m$

Step3.4.2.1 $\text{Log}_a b \leftarrow (mj - i) \bmod n$ 结束

Step3.4.3 else go to Step3.4.1

算法成功停机的充要条件是 $b \in \langle a \rangle$，$\langle a \rangle$ 为由 a 生成的群。

必要性:成功停机说明算法 2 的 Step3.3.2.1 或者 Step3.4.2.1 中的等式 $(L_3(j))^m = b \cdot L_4(i)$ 成立,也即等式 $a^{mj} = y = ba^i$ 成立,则 $b = a^{\langle mj-i \rangle}$，由于 $1 \leqslant i,j \leqslant m$，有 $0 \leqslant mj - i$，又 a 是生成元,所有 $b \in \langle a \rangle$。

充分性:因为 $b \in \langle a \rangle$，$0 \leqslant \log_a b \leqslant n - 1$，$m = \lceil n^{\frac{1}{2}} \rceil$，所以 $0 \leqslant \log_a b \leqslant n - 1 \leqslant m^2 - 1$。令 $1 \leqslant i \leqslant m$ 且 $\log_a b = mj - i$，则可知 $1 \leqslant i \leqslant m$。当 i,j 满足 $1 \leqslant i,j \leqslant m$ 时，$\log_a b$ 可以写成 $\log_a b = mj - i$。a 是生成元，有 $b = a^{\langle mj-i \rangle}$，即 $a^{mj} = ba^i$，则算法 2 的 Step3.3.2.1 或者 Step3.4.2.1 一定可以成功,所以算法 2 可以成功停机。

4　改进算法的性能分析

根据群乘法为基本运算单位,分析改进的算法的时间空间复杂性。

在 Step1 预处理中,算法根据结束条件计算出 (i,j) 对的奇偶分组,时间复杂度为 $O(n)$，空间复杂度为 $O(n/2)$，相比算法 1 此步骤的复杂度上相对较大,考虑到算法的效率问题,这一步可以在计算之前预先做好,对于相同的 n 条件下,不同的生成元所产生的奇偶链表是相同的,即在不改变 n 的情况下,得到的奇偶链表可以提供给同一群的不同生成元求解离散对数问题。

在 Step2 中把高阶的幂指数利用较小的海明权重形式表示,在计算高阶幂运算中可以减少乘法的次数,显著提高算法的运算速度,提高的效率在 11% 左右,并且 Step2.2 中不需要计算 a^m，提高了该算法的计算效率和存储空间。

在 Step3.1 中,首先计算 a 的各次幂值,然后通过 Step3.3 判断结果值 $\log_a b$ 的奇偶性，根据判断结果的奇偶性,利用预处理中得到的奇偶 (i,j) 对,只需遍历 (i,j) 对中的奇数对链表或者偶数对链表,利用 (i,j) 对直接验证得到结果,时间复杂度为 $O(n/4)$，同时不需要利用哈希表来对结果进行处理,直接查表即可,查表时间为 $O(1)$。

在 Step3.3 和 Step3.4 中利用多精度平方乘算法可以提高运算速度,同时利用事先计算的 a 的各次幂值,直接查询即可参与多精度平方乘运算,查表时间为 $O(1)$。

随着计算机发展的不断提高,计算机的计算能力和计算机硬件的配置已经有了很大的进步,随着计算机的普及和性能上的提升,以前相对较复杂的算法已经逐步得到了改善和优化,同时对于一个算法而言,空间的消耗对于一个算法的权重越来越小,相对于空间复杂度,算法的时间复杂度的提升显的更加重要。在计算效率上的提升是一个好的算法的重要指标。

5　算法对比分析

根据上面的算法分析,可以总结出以上两个算法的不同之处。

1)预处理过程。算法 1 没有预处理过程,而算法 2 在预处理过程中产生了 2 个根据判定条件得到的奇偶链表,并且该奇偶链表在 m 值没有改变的情况下可以重复使用,可以减少在 m 值相同时的重复计算过程,提高了代码的重用性和计算结果的利用率,并利用其来求解同群下不同生成元的离散对数问题。

2)求逆操作。算法 1 在计算中需要先计算 a^{-1} 并

缓存,而算法 2 中不需要求逆操作,因此算法 2 在计算效率上更高。

3)高次幂运算。算法 1 中在计算高次幂中利用平方乘算法计算,而在算法 2 中的处理是首先利用较小的海明权重表示法表示幂指数,减少了幂运算中的乘法次数,然后再利用多精度平方乘算法进行相应的高次幂计算,该算法比平方乘算法计算效率更高,在高次幂运算步骤中可以更快地计算得到相应的结果。

4)表元素的查找次数。算法 1 中的 Step2 和算法 2 中的 Step3.1 的计算量是一样的,而算法 1 在比较过程中需要进行查表比较,最大计算量在 $O(n)$,平均计算量是 $O(n/2)$;而算法 2 利用预处理过程中得到的范围,只需直接查找,最大计算量为 $O(n/4)$,平均下来计算量仅有 $O(n/8)$ 。在算法运算次数上有倍数的降低。

5)链表的处理。算法 1 在对链表处理时使用哈希函数来得到无碰撞的值,而在算法 2 中利用生成元的性质可知在小于群的阶范围内, a^i 是无碰撞的,所以算法 2 不需要使用哈希函数。也就在查表过程中可以提高效率,这在性能上也是一个提升。

表 1 为原算法与改进算法对比。

表 1 原算法与改进算法对比

比较内容	算法 1	算法 2
预处理	a^m	(i,j) 奇偶对,并且在求解同一群的其他生成元的离散对数问题时可以重复使用
求逆操作	$O(\log n)$	无
奇偶判断	无	减少 $\frac{3}{4}$ 的运算量
比较次数	平均 $O(n/2)$	平均 $O(n/8)$
查表时间	$O(m)$	$O(1)$

6 进一步的应用

通过求解某一群中的离散对数问题,利用在求解过程中所得到的中间数据,可以加以分析和利用,对同群下其他生成元的离散对数的求解问题进行分析。根据算法 2 的中心思想,发现算法 2 中预处理过程中是利用群的阶作为输入参数,和生成元的选取无关,利用这个特征,可以利用算法 2 中预处理过程中的数据对离散对数问题的求解简化处理。

考虑在同一群下其他生成元的离散对数的问题,可以重复利用算法 2 中预处理过程中得到的 (i,j) 对奇偶链表,针对同一群下的其他生成元,群的阶是不变的,则根据算法 2 可知其他生成元所对应的 (i,j) 对都是相同的,根据定理 1 可知在求解同一群下其他生成元的离散对数情况时,可以直接利用算法 2 中得到的 (i,j) 对来进行计算,通过这一方法可以减少算法 2 的预处理过程,降低算法的运算量。

7 结束语

文中针对小步大步算法与改进的算法进行了性能上的分析,上述表明算法的改进是正确可行的。随着硬件条件的日益强大,牺牲适当的存储空间来降低计算的复杂度,提高算法的效率也是一种可行的方案。加大代码的重用率、有效利用中间过程产生的数据来简化计算过程也是在日后密码系统的实现过程中需要考虑和探讨的问题。

参考文献:

[1] Johannes B, Damian W. Discrete logarithms: recent progress [C]//International Conference on Coding Theory, Cryptography and Related Areas. Berlin: Springer-Verlag, 2000: 42-56.

[2] Douglas R S. Cryptography theory and practice[M]. 2nd ed. 冯登国,译. 北京:电子工业出版社,2003:193-227.

[3] Mao Wenbo. 现代密码学理论与实践[M]. 王继林,译. 北京:电子工业出版社,2004.

[4] 周玉洁,冯登国. 公开密钥密码算法及其快速实现[M]. 北京:国防工业出版社,2002.

[5] 王 晚,杜伟章. 基于离散对数问题的多级代理盲签名方案[J]. 计算机应用,2011,31(7):1904-1905.

[6] 欧海文,叶顶峰,杨君辉,等. 关于同时基于因子分解与离散对数问题的签名体制[J]. 通信学报,2004,25(10):143-147.

[7] 李发根,辛向军,胡予濮. 基于离散对数和因子分解签名方案的改进[J]. 中国铁道科学,2006,27(5):132-135.

[8] 张海波,王小非,夏学知,等. 一个改进的离散对数问题攻击算法[J]. 计算机应用,2007,27(4):843-845.

[9] 胡 进,何德彪,陈建华,等. 基于椭圆曲线同源的公钥密码体制[J]. 北京工业大学学报,2011,37(6):916-920.

[10] 阎军智,李凤华,马建峰. 基于 Diffie-Hellman 算法的分层密钥分配方案[J]. 电子学报,2011,39(1):119-123.

[11] Muir J A, Stinson D R. On the low hamming weight discrete logarithm problem for nonadjacent representations [J]. AECC, 2006, 16(6): 461-472.

[12] Menezes A J, van Oorschot P C, Vanstone S A. Handbook of applied cryptography[M]. 胡 磊,王 鹏,译. 北京:电子工业出版社,2005.

离散对数问题攻击算法的改进

作者： 汤鹏志， 何涛， 李彪
作者单位： 华东交通大学 基础科学学院,江西 南昌330013
刊名： 计算机技术与发展
英文刊名： Computer Technology and Development
年，卷(期)： 2013(5)