

文章编号:1001-9081(2007)04-0843-03

一个改进的离散对数问题攻击算法

张海波^{1,2}, 王小非^{1,2}, 夏学知², 黄友澎^{1,2}

(1. 哈尔滨工程大学 计算机科学与技术学院, 黑龙江 哈尔滨 150001;

2. 武汉数字工程研究所, 湖北 武汉 430074)

(zhanghb412@yahoo.com.cn)

摘要: 小步一大步攻击算法是一个求解离散对数问题通用且高效的算法, 但较大的存贮开销是它的一个明显不足。提出的改进算法使得存贮开销减少一半, 并取消了求逆元操作, 通过引入抗冲突的哈希函数, 省略了表排序过程, 并使查表时间降到常数级。性能分析表明, 改进算法的时间和空间耗费明显降低, 性能优于原算法。另外, 还探讨了如何通过降低问题的规模来进一步缩短攻击算法的计算过程, 并给出了一个简单易行的对离散对数进行奇偶筛选的方法。

关键词: 离散对数问题; 小步一大步攻击算法; 成功停机; 平方乘算法

中图分类号: TP309 **文献标识码:** A

An improved attack algorithm for discrete logarithm problem

ZHANG Hai-bo^{1,2}, WANG Xiao-fei^{1,2}, XIA Xue-zhi², HUANG You-peng^{1,2}

(1. School of Computer Science and Technology, Harbin Engineering University, Harbin Heilongjiang 150001, China;

2. Wuhan Digital Engineering Institute, Wuhan Hubei 430074, China)

Abstract: Baby-step-giant-step attack algorithm is universally suitable to solve all discrete logarithm problems, but its relatively larger storage cost is an obvious defect. An improved attack algorithm which can cut down half of space spending and cancel the inversing-computation on multiplicative group was presented. By using hash function, this new algorithm abolishes list-sorting process and drops the time complexity of list-searching into O(1). The performance analysis shows that the new algorithm obviously reduces the time and space use. Furthermore, how to play down the input size to shorten computation journey of attack algorithms was discussed and an easy way to parity sieve for discrete logarithm was given.

Key words: Discrete Logarithm Problem (DLP); baby-step-giant-step attack algorithm; successfully termination; square-multiplication algorithm

很多密码技术的安全性都建立在离散对数问题的困难性上, 如 Diffie-Hellman 密钥协议^[1], ElGamal 密码体制及其签名方案, 以及它们的变种等。Diffie-Hellman 问题^[2], 模合数 n 乘群 Z_n^* 中的离散对数问题, 以及 n 的因子分解问题, 在密码学上存在一定的关联, 它们的困难性存在着内在的等价性^[1]。

针对离散对数问题有许多攻击方法, 目前已知的有穷举攻击, Pohlig-Hellman 攻击^[3], 指数积分攻击^[3], Pollard 概率攻击^[3], 小步一大步攻击^[2,4], 袋鼠攻击^[5]和生日攻击^[6]等。这些攻击方法往往在某些特定场合尤其有效, 如当 $p-1$ 为形如 2 的幂次方^[6], $p-1$ 的因数都较小^[3] 或 p 的位数较短时。小步一大步攻击算法则适合于包括椭圆曲线^[2,3]在内的所有离散对数问题, 是本文进行研究并加以改进的对象。

对于小步一大步攻击算法, 在忽略对数因子的情况下, 其时间复杂度为 $O(\sqrt{n})$, 已接近于离散对数问题的任何通用算法的复杂性下界^[6], 但仍留有值得优化的余地。另一方面, 空间复杂度较大一直是小步一大步算法的不足之处。

1 离散对数问题

在密码学系统中, 一般将求解数论中某个数的对数的问

题称为离散对数问题 (Discrete Logarithm Problem, DLP)。

定义 1 设 (G, \cdot) 是乘法群, 对于一个 n 阶元素 $\alpha \in G$ 和元素 $\beta \in \langle \alpha \rangle$, 存在唯一的整数 $a, 0 \leq a \leq n-1$, 满足: $\alpha^a = \beta$, 称 a 为 α 与 β 相关的离散对数, 记为 $\log_{\alpha}\beta$ 。

密码学领域内的离散对数问题是困难的^[2~4], 即计算上不可行。这是许多密码技术的安全性之所在。下面的命题进一步阐明了离散对数问题保持安全性的一个性质。

命题 1 离散对数问题的困难性与其生成元的选取无关。

证明 设 α 和 γ 是阶为 n 的乘法群 G 的两个不同生成元, 且设 $\beta \in G$ 。若 $x = \log_{\alpha}\beta, y = \log_{\gamma}\beta, z = \log_{\alpha}\gamma$, 则有 $\alpha^x = \beta = \gamma^y = (\alpha^z)^y$ 。从而有 $x = zy \bmod n, \log_{\gamma}\beta = \log_{\alpha}\beta(\log_{\alpha}\gamma)^{-1} \bmod n$ 。这表明任何计算以为 α 底的对数的算法, 也可以用于计算以 G 的其他生成元 γ 为底的对数。

对于群论, 密码学上应用最广泛的有两类, 一类是有限域 F_q 上的乘群 F_q^* 。如模素数 p 的乘群 Z_p^* , 有限域 F_{2^m} 上的乘群 $F_{2^m}^*$, 以及 n 为合数的乘群 Z_n^* 。另一类是定义在有限域上的椭圆曲线的点群。适用于乘群上的离散对数算法, 只要稍作修改均可直接应用到基于椭圆曲线的离散对数问题, 故本文侧重

收稿日期: 2006-09-30; 修订日期: 2007-01-05

作者简介: 张海波(1972-), 男, 湖北人, 博士研究生, 主要研究方向: 密码学、信息安全; 王小非(1957-), 男, 湖北人, 研究员, 博士生导师, 主要研究方向: 网络、信息安全、并行计算; 夏学知(1966-), 男, 湖北人, 研究员, 博士, 主要研究方向: 网络与信息栅格、并行计算; 黄友澎(1963-), 男, 福建人, 博士研究生, 主要研究方向: 数据融合、信息安全。

于讨论乘群上的离散对数。

离散对数的求解虽是困难的,但其逆运算即指数运算,可以应用平方乘的方法有效地计算。若将指数用有符号的二进制数表示,使之具有较小的海明权重^[7],则可以进一步减少其中乘法的次数,从而提高运算速度。

2 小步一大步攻击算法及分析

小步一大步(Baby-Step-Giant-Step)攻击算法有时也称为Shanks 算法^[4],具体实现如下面的算法 1 所示。其中参数 n , α, β 的意义与定义 1 中的定义相同。

算法 1 小步一大步攻击算法^[2]

Baby-Step-Giant-Step(n, α, β)

- 1) $m \leftarrow \lceil \sqrt{n} \rceil$
- 2) for $j \leftarrow 0$ to $m - 1$
 - (2.1) 计算 α^{mj}
- 3) 对 m 个有序对 (j, α^{mj}) 关于第二个坐标排序, 得到一个列表 L_1
- 4) for $i \leftarrow 0$ to $m - 1$
 - (4.1) 计算 $\beta\alpha^{-i}$
- 5) 对 m 个有序对 $(i\beta\alpha^{-i})$ 关于第二个坐标排序, 得到一个列表 L_2
- 6) 找到 $(j, y) \in L_1$ 和 $(i, y) \in L_2$ (即找到两个具有相同第二坐标的有序对)
- 7) $\log_\alpha \beta \leftarrow (mj + i) \bmod n$

下面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性。

在第 2) 步,为了(2.1)步计算的快速,要先预计计算 α^m 并缓存,平方乘算法是比较通用且非常有效的方法,比单纯的连乘算法提速显著,采用平方乘算法也需要 $O(\log m)$;另外,第(2.1)步需执行 m 次,时间开销是 $O(m)$ 。

在第 3) 步,若用快速排序算法,也得 $O(m \log m)$ 。同样,第 5) 步的时间复杂度也为 $O(m \log m)$ 。在这两步中,分别需 $O(m)$ 的空间复杂度。

在第 4) 步,为了(4.1)步的快速计算,需先计算 $\alpha - 1$ 并缓存,采用扩展的 Euclidean 算法,时间复杂度为 $O(\log \alpha) \approx O(\log m)$;另外,第(4.1)步需执行 m 次,时间开销是 $O(m)$ 。

由于列表 L_1 和 L_2 已经排好序,第 6) 步的查找时间为 $O(m)$ 。

综上所述,算法 1 的总的时间复杂度为 $O(m \log m)$,空间复杂度为 $O(m)$ 。若忽略对数因子,时间和空间复杂度均为 $O(m) = O(\sqrt{n})$ 。

进一步研究算法 1 可发现,小步一大步攻击算法能否正确地返回所求解的离散对数,关键在于第 6) 步能否成功。通过下面的命题作进一步的阐述。

命题 2 小步一大步攻击算法成功停机的充要条件是 $\beta \in < \alpha >$

证明

1) 必要性。算法 1 成功停机,表明第 6) 步有 $\alpha^{mj} = y = \beta\alpha^{-i}$, 则 $\beta = \alpha^{(mj+i)}$, α 是生成元,故 $\beta \in < \alpha >$ 。

2) 充分性。 $\beta \in < \alpha >$, 可令 $\beta = \alpha^x$, 则 $x = \log_\alpha \beta$, 因 $\alpha \in G$ 的阶为 n , 且 $m = \lceil \sqrt{n} \rceil$, 有 $0 \leq \log_\alpha \beta \leq n - 1$, 故可令 $i = \log_\alpha \beta \bmod m$, 从而可令 $\log_\alpha \beta = mj + i$, 又 $\log_\alpha \beta \leq n - 1 \leq m^2 - 1 = m(m - 1) + m - 1$, 故有 $0 \leq i, j \leq m - 1$ 。由 $\log_\alpha \beta = mj + i$, α 是生成元, 有 $\beta = \alpha^{(mj+i)}$, 即 $\alpha^{mj} = \beta\alpha^{-i}$, 故第 6) 步必会成功,从而算法会成功停机。

3 改进算法

先给出改进后的算法描述,其中参数与算法 1 完全相同。

算法 2 改进的小步一大步攻击算法 Improved-Baby-Step-Giant-Step (n, α, β)

- 1) 系统初始化
 - (1.1) $s \leftarrow 1, u \leftarrow \beta, L_1 \leftarrow \text{Null};$
 - (1.2) $m \leftarrow \lceil \sqrt{n} \rceil$, m 转换成具有较小海明权重^[7] 的表示形式;
 - (1.3) 运用多精度平方乘^[1] 算法计算 $\alpha^m, t \leftarrow \alpha^m$;
- 2) for $j \leftarrow 1$ to m
 - (2.1) $s \leftarrow s \times t;$
 - (2.2) $L_1(h(s)) \leftarrow (j, s)$, 其中 $h()$ 是抗冲突的哈希函数
- 3) for $i \leftarrow 1$ to m
 - (3.1) $u \leftarrow u \cdot \alpha;$
 - (3.2) 若 $L_1(h(u)) = (j, y) \neq \text{NULL}$, $\log_\alpha \beta \leftarrow (mj - i) \bmod n$, 结束。

命题 3 算法 2 成功停机的充要条件是 $\beta \in < \alpha >$ 。

证明

1) 必要性。算法 2 成功停机,表明第(3.2)步有 $\alpha^{mj} = y = \beta\alpha^i$, 则 $\beta = \alpha^{(mj-i)}$, 因 $1 \leq i, j \leq m$, 有 $mj - i \geq 0$, 又 α 是生成元,故 $\beta \in < \alpha >$ 。

2) 充分性。 $\beta \in < \alpha >$, $0 \leq \log_\alpha \beta \leq n - 1, m = \lceil \sqrt{n} \rceil$, 故 $0 \leq \log_\alpha \beta \leq n - 1 \leq m^2 - 1$ 。令 $1 \leq j \leq m$ 且 $\log_\alpha \beta = mj - i$, 则易知 i 满足: $1 \leq i \leq m$ 。也即当 i, j 满足 $1 \leq i, j \leq m$ 时, $\log_\alpha \beta$ 可写成 $\log_\alpha \beta = mj - i$ 。 α 是生成元, 有 $\beta = \alpha^{(mj-i)}$, 即 $\alpha^{mj} = \beta\alpha^i$, 故算法 2 第(3.2)步必会成功,从而算法 2 会成功停机。

从命题 3 的证明过程可知,改进后的算法 2 是一个能返回正确结果的有效算法。

4 改进算法的性能分析

同样以群乘法为基本运算单位,分析改进算法的时间和空间复杂性。

与算法 1 一样,在第 1) 步,要先预计计算 α^m 并缓存。虽时间复杂度仍为 $O(\log m)$,但在(1.2)步中将指数 m 采取具有较小海明权重^[7] 的表示方式,可以显著减少其中乘法的次数,从而可以平均提高大致 11% 的运算速度^[2]。由于平方运算最快可以比两个不同整数的乘法运算快两倍^[1],所以这项措施的好处是非常明显的;同时在(1.3)步中采用多精度平方乘算法^[1],可进一步提高运算速度。

在第(2.2)步,无须排序操作,只需通过抗冲突的哈希函数快速建立索引表,且仅需一张表 L_1 ,省略了第二张表 L_2 ,也即存贮空间减少了一半。

在第(3.2)步,哈希函数的引入使得查表时间降为 $O(1)$ 。

随着计算能力的不断提升,目前要求素数 p 的取值一般都在 1024 bit 或更长,故一次快速哈希函数的时间相对于一次两个 1024 bit 大整数相乘的时间来说微不足道,可以近似不计。同时 p 的取值要求(1024 bit 或更长)也表明改进算法的时间和空间优势是比较显著的。

5 两算法的对比

由上面的分析,可归纳出两个算法的主要不同之处在于:

1) 存贮表的数目。算法 1 需要两个表,而算法 2 则只需 1 个,从而存贮器开销不同。

2) 表元素的比较时机。算法 1 是两组数据(两张表)都

计算完成后再进行比较,而算法2则是只需在第一张表完成的基础上即可开展比较工作。

3)求解成功时的条件和结果的计算公式。算法1求解成功时有 $\alpha^{mj} = y = \beta\alpha^{-i}, 0 \leq i, j \leq m - 1$,结果为 $\log_{\alpha}\beta = (mj + i) \bmod n$ 。而算法2求解成功时则是 $\alpha^{mj} = y = \beta\alpha^i, 1 \leq i, j \leq m$,结果为 $\log_{\alpha}\beta = (mj - i) \bmod n$ 。

4)是否需要求解逆元。算法1需要求解逆元,而算法2则无需求解任何逆元。

5)表排序与查表时间。算法1需对两张表都排序,且查表时间与表的规模直接相关(为 $O(m)$)。而算法2由于引入抗冲突的哈希函数,无须排序操作,且查表时间也降为 $O(1)$ 。

表1 改进算法与原算法的性能对比

比较项目	原算法	改进算法
预算算 α^m	采用平方乘算法	采用具有较小海明权重指数的多精度平方乘算法,运算速度提高约11%
预算算 α^{-1}	采用扩展的Euclidean算法, $O(\log\alpha) \approx O(\log m) *$	无
缓存	需存 α^m 和 α^{-1}	只需存 α^m
表1元素计算时间	m 次群乘法	相同
表2元素计算时间	m 次群乘法	平均 $(m+1)/2$ 次群乘法 **
表排序	两个表,每个表各 $O(m\log m)$	无
查表时间	$O(m)$	$O(1)$
需存贮的元素数目	$2m$	m

注: * $m = \lceil \sqrt{n} \rceil$, n 为元素 $\alpha \in G$ 的阶。

**当查找成功时所需的平均计算时间为 $= \sum_{i=1}^m i \cdot \left(\frac{1}{m}\right) = \frac{m+1}{2}$ 次群乘法。

6 进一步的改进措施

改进后的小步一大步攻击算法较原算法而言进行了算法实现上的多项优化,但这仅是针对算法本身的优化,两种算法所面对的问题规模仍然是相同的。可以尝试通过降低问题的规模来进一步缩短攻击算法的计算过程。这一点对于比特位较长的素数 p 意义更加明显。

(上接第842页)

图2是语音信号隐藏秘密信息前后的波形图,图3是语音信号隐藏秘密信息前后的频谱图。从主观听觉测试结果表明,本文所提算法获得的携密语音仅仅比原始明文略多一点噪声,并不影响整体听觉效果。在长度为4.109s(样点总数约为 9.1×10^4)的语音数据中嵌入了2964bit的信息。从图中可以看出秘密信息嵌入后没有引起语音信号质量大的变化。

5 结语

本文基于一般语音编码对相邻段语音能量比改变不大这一特性,提出了一种能够在GSM移动通信网络中使用的信息隐藏算法能量比调整(ABS Energy Ratio Adjust)算法。算法采用了ABS技术,在隐藏算法中根据输入明文语音实时的调整相邻段能量比,使得隐藏效果和解码效果都达到最佳值。

一个较易快速实现的措施就是对将要计算的 $\log_{\alpha}\beta$ 先进行奇偶筛选,这样可以将问题的规模降低约一半。该措施的有效性和奇偶筛选的实现方法由下面的命题4给出。其中 n, α, β 的意义同定义1,且定义在模 p 的乘群 Z_p^* 上。

命题4 若 $\beta^{n/2} = 1 \bmod p$,则 $\log_{\alpha}\beta$ 是偶数,否则是奇数。

证明 设 $x = \log_{\alpha}\beta \bmod n$,则 $\beta = \alpha^x \bmod p$ 。有 $(\alpha^{n/2})^2 = \alpha^n = 1 \bmod p$,则 $\alpha^{n/2} = \pm 1 \bmod p$ 。因 α 的阶为 n ,有 $\alpha^{n/2} \neq 1 \bmod p$,故 $\alpha^{n/2} = -1 \bmod p$ 。从而 $\beta^{n/2} = \alpha^{x \cdot n/2} = (-1)^x \bmod p$ 。也即 $\beta^{n/2} = 1 \bmod p$ 时 $\log_{\alpha}\beta$ 是偶数,否则是奇数。

7 结语

本文将改进后的小步一大步攻击算法与原算法的性能进行了对比分析,表明上述改进措施均是正确而行之有效的。如何减少存贮开销,尽量避免或减少求逆元运算,如何有效应用多精度算法,以及通过变换指数表现形式来加速幂运算速度等,都值得在日益广泛应用的密码系统和签名方案的实现过程中加以充分考虑和探讨。

努力提高攻击算法的运算效率只是一个方面的工作,延伸到如何降低算法的输入规模将是一件非常有意义的工作。本文仅讨论了离散对数的奇偶筛选问题,如何预测或确定离散对数中的其他多个特定比特位的数值值得进一步的深入研究。

参考文献:

- [1] ALFRED JM, PAUL CVO, SCOTT AV. Handbook of applied cryptography[M]. 胡磊, 王鹏, 译. 北京: 电子工业出版社, 2005. 99 - 101, 459 - 468, 527 - 532.
- [2] DOUGLAS RS. Cryptography theory and practice. Second edition [M]. 冯登国, 译. 北京: 电子工业出版社, 2003. 193 - 227.
- [3] JOHANNES B, DAMIAN W. Discrete logarithms: recent progress [A]. International Conference on Coding Theory, Cryptography and Related Areas[C]. Berlin: Springer-Verlag, 2000. 42 - 56.
- [4] ANDREW O. Discrete logarithms: the past and the future[J]. Designs, Codes, and Cryptography, 2000, 19(2/3): 129 - 145.
- [5] CHRIS S. The discrete log problem[D]. PhD. Thesis, University of Toronto, 2002. 7 - 9.
- [6] WADE T, LAWRENCE CW. Introduction to cryptography with coding theory[M]. 邹红霞, 许鹏文, 李勇奇, 译. 北京: 人民邮电出版社, 2004. 121 - 122, 127 - 134.
- [7] MUIR JA, STINSON DR. On The low hamming weight discrete logarithm problem for nonadjacent representations[J]. AAECC, 2006, 16(6): 461 - 472.

大量仿真试验结果表明,算法对GSM中的RPE2LTP编码有很强的鲁棒性。算法简单易行并且是基于盲检测的,具有很大的实用性。本文提出的基于语音的信息隐藏方法可以广泛运用于移动通信网条件下信息安全传输、数字水印等领域。

参考文献:

- [1] 陈力, 谢玉琼. 一种基于分形维数的自适应语音信息隐藏算法[J]. 武汉大学学报, 2003, 49(3): 313 - 317.
- [2] 郑见灵, 谭月辉, 焦桂芝, 等. 音频文件中信息隐藏技术研究及其实现[J]. 河北工业科技, 2006, 23(2): 76 - 79.
- [3] WU ZJ, YANG W, YANG YX. ABS-based speech information hiding approach[J]. Electronics Letters, 2003, 39(22): 1617 - 1619.
- [4] 吴志军, 钮心忻, 杨义先, 等. 语音隐藏的研究及实现[J]. 通信学报, 2002, 23(8): 99 - 104.