On the computation of discrete logarithms in class groups

Extended abstract

Johannes Buchmann
Stephan Düllmann
FB14-Informatik
Universität des Saarlandes
D-6600 Saarbrücken
West Germany

July 29, 1993

On the computation of discrete logarithms in class groups

Extended abstract

1 Introduction

In [3] and [1] a new key exchange system was introduced whose security is related to the difficulty of solving the discrete logarithm problem in the class group of imaginary quadratic orders. Subsequently, in [5] and [4] a subexponential algorithm for computing those class groups was presented and it was shown how to use this algorithm and the index-calculus method to calculate discrete logarithms.

In this paper we show how the output of the class group algorithm can be used to simplify the index-calculus algorithm in class groups considerably. This simplification enables us to use a slight modification of our implementation [2] of the algorithm of Hafner and McCurley to calculate discrete logarithms in fairly large class groups. At the end of the paper we will present the results of some experiments which show that the computation of discrete logarithms in class groups is very easy once the class group has been computed by the subexponential algorithm.

2 The idea

Let G be a finite abelian group. Let

$$G = < \gamma_1 > \times \ldots \times < \gamma_l > \tag{1}$$

be a presentation of G as a direct product of cyclic groups. Suppose for $\alpha, \beta \in G$ we wish to find $x \in \mathcal{Z}$ with

$$\alpha^x = \beta. \tag{2}$$

The method we suggest is very simple: Calculate the representations

$$\alpha = \prod_{i=1}^{l} \gamma_i^{a_i} \; , \beta = \prod_{i=1}^{l} \gamma_i^{b_i} .$$

Then (2) implies

$$\prod_{i=1}^{l} \gamma_i^{x \cdot a_i} = \prod_{i=1}^{l} \gamma_i^{b_i}$$

which is solvable if and only if the system of simultaneous congruences

$$x a_i \equiv b_i \mod g_i \qquad (1 \leq i \leq l) \tag{3}$$

where $g_i = | < \gamma_i > |$ $(1 \leq i \leq l)$ has a solution. This system can be solved by means of the generalized chinese remainder theorem.

3 Application to class groups

Let Cl be the class group of an imaginary quadratic order of discriminant D. The algorithm of Hafner and McCurley starts from a generating set $\{\mathcal{P}_1, \ldots, \mathcal{P}_k\}$ for Cl and subsequently calculates a basis $\{\underline{b}_1, \ldots, \underline{b}_k\} \subseteq \mathcal{Z}^k$ for the relation lattice

$$L = \left\{ \underline{e} = (e_1, \ldots, e_k) \in \mathcal{Z}^k \colon \prod_{i=1}^{k} \mathcal{P}_i^{e_i} = 1 \right\} .$$

Then the Smith normal form

$$S = \text{diag } (g_1, \ldots, g_l, 1, \ldots, 1) \in \mathcal{Z}^{k \times k}$$

of $B = (\underline{b}_1, \ldots, \underline{b}_k)$ is calculated, $(g_l > 1)$,

$$S = U^{-1} B V$$

with $U, V \in \mathrm{GL}\,(k, \mathcal{Z})$. The transformation matrices U and U^{-1} are also output of the algorithm. If we put $U = (u_{ij})_{k \times k}$ and

$$G_i = \prod_{j=1}^{k} \mathcal{P}_j^{u_{ij}} \qquad (1 \leq i \leq l) \tag{4}$$

then

$$Cl = < G_1 > \times \ldots \times < G_l >$$

and

$$| < G_i > | = g_i \qquad (1 \leq i \leq l).$$

Conversely, if we let $U^{-1} = (u'_{i,j})_{k \times k}$ then we have

$$\mathcal{P}_i = \prod_{j=1}^{l} G_j^{u'_{i,j}} \qquad (1 \leq i \leq k) \tag{5}$$

Moreover, if we are given a representation of an element in the class group on the generating system $\{\mathcal{P}_1, \ldots, \mathcal{P}_k\}$, then we can use (5) to come up with a representation of that element on the generating system $\{G_1 \ldots, G_l\}$.

Now suppose that we want to solve

$$A^x = B$$

in Cl. In order to apply the ideas of the previous section it is sufficient to determine representations

$$A = \prod_{i=1}^{k} \mathcal{P}_i^{a'_i} \ , \ B = \prod_{i=1}^{k} \mathcal{P}_i^{b'_i} \tag{6}$$

since those can be transformed into presentations

$$A = \prod_{i=1}^{l} G_i^{a_i} \ , \ B = \prod_{i=1}^{l} G_i^{b_i}. \tag{7}$$

But those presentations are computed as follows: Let $\wp_1, \ldots, \wp_k$ be first degree prime ideals such that $\mathcal{P}_i$ is the equivalence class of $\wp_i$ $(1 \leq i \leq k)$ and let $\mathcal{A}$ be the reduced ideal in the class of A. For random exponent vectors $\underline{v} = (v_1, \ldots, v_k) \in [0, \ldots D-1]^k$ we calculate the reduced ideal $\mathcal{A}'$ in the class of $\mathcal{A} \prod_{i=1}^{k} \wp_i^{v_i}$ until we find such an $\mathcal{A}'$ which can be written as $\mathcal{A}' = \prod_{i=1}^{k} \wp_i^{v'_i}$. Then

$$\mathcal{A} = \prod_{i=1}^{k} \wp_i^{v'_i - v_i}$$

is the presentation we were looking for. Analogeously, we can find such a representation for a reduced ideal $\mathcal{B}$ in the class of B. If we use all the prime ideals whose norm is bounded by $L[\beta]$ where for $\beta > 0$ we use the notation

$$L[\beta] = \left(\exp\sqrt{\log D \log\log D}\right)^{\beta+o(1)}$$

as usual then each trial takes time $L[0]$ and the probability for being able to factor $\mathcal{A}'$ is $L\left[-\frac{1}{4\beta}\right]$. So the expected running time of the procedure that finds the representation on the original generating system takes time $L[\frac{1}{4\beta}]$. The computation of the representation on the generating system $\{G_1, \ldots, G_l\}$ can be carried out in time $L[\beta]$. The optimal value for β is $\beta = \frac{1}{2}$. Hence the expected running time for each new discrete logarithm problem is $L\left[\frac{1}{2}\right]$.

4 Numerical results

In the tables below we present the results of some experiments concerning the computation of discrete logarithms in class groups of imaginary quadratic fields. In the first table we give the following data:

- discriminant D,
- size k of the generating set $\{\mathcal{P}_1, \ldots, \mathcal{P}_k\}$,
- size l of the generating system $\{G_i, \ldots G_l\}$,
- values of g_i $(1 \leq i \leq l)$,
- class number h.

D	k	l	h	$g_i (1 \leq i \leq l)$
$-(4 \cdot 10^{24} + 4)$	1404	3	1 154 987 161 920	2, 4, 144 373 395 240
$-(4 \cdot 10^{29} + 4)$	1902	3	436 605 442 139 682	2, 2, 109 151 360 534 920
$-(4 \cdot 10^{34} + 4)$	2609	4	189 652 590 177 168 096	2, 2, 2, 23 706 573 772 146 012
$-4 \cdot F_7$	3257	2	17 787 144 930 223 461 408	2, 8 893 572 465 111 730 704

$(4 \cdot F_7 = 4 \cdot (2^{2^7}+1) = 1\ 361\ 129\ 467\ 683\ 753\ 853\ 853\ 498\ 429\ 727\ 072\ 845\ 828)$

In the second table we present the running times for the several stages of the algorithm. All timings given here are seconds CPU-time on a Sun 4/60-Sparc Station 1.

- time t_1 to compute the sets $\{G_1, \ldots, G_l\}, \{g_1, \ldots, g_l\}$, the transformation matrices U and V and the class number h using our implementation [2].
- time t_2 to determine the representations (6) for given A and B,
- time t_3 to transform the representation (6) for given A and B into the presentation (7).
- time t_4 to solve the simultaneous congruences (3).

Note that t_2, t_3 and t_4 are very small compared to t_1 and so the effort for each new discrete logarithm problem in the same field is quite small.

D	t_1	t_2	t_3	t_4
$-(4 \cdot 10^{24} + 4)$	3418	5	4	< 1
$-(4 \cdot 10^{29} + 4)$	18 587	21	5	< 1
$-(4 \cdot 10^{34} + 4)$	123 404	37	10	< 1
$-4 \cdot F_7$	511 978	96	18	< 1

References

[1] J. Buchmann, S. Düllmann, H.C. Williams, *On the complexity and efficiency of a new key exchange system*, Proceedings EUROCRYPT'89, to appear.

[2] J. Buchmann, S. Düllmann, *A probabilistic class group and regulator algorithm and its implementation*, Proceedings Colloquium on Computational Number Theory, Debrecen 1989, to appear.

[3] J. Buchmann, H.C. Williams, *A key exchange system based on imaginary quadratic fields*, J. Cryptology **1** (1988), 107-118.

[4] J.L. Hafner, K.S. McCurley, *A rigorous subexponential algorithm for computation of class groups*, Journal AMS, to appear.

[5] K.S. McCurley, *Cryptographic key distribution and computation in class groups*, Proceeding of NATO ASI Number Theory and Applications, Kluwer Academic Publishers 1989, 459-479.