Cryptanalysing the Critical Group

Simon R. Blackburn
Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX
United Kingdom
s.blackburn@rhul.ac.uk

April 15, 2008

Abstract

Biggs has recently proposed the critical group of a certain class of finite graphs as a platform group for cryptosystems relying on the difficulty of the discrete log problem. The paper uses techniques from the theory of Picard groups on finite graphs to show that the discrete log problem can be efficiently solved in Biggs's groups. Thus this class of groups is not suitable as a platform for discrete log based cryptography.

1 Introduction

Let G be an abelian group written additively, and let $g, h \in G$ have the property that h lies in the subgroup generated by g. The *discrete log problem* asks for an integer k such that $h = kg$. Of course, the difficulty of the discrete log problem depends heavily on the representation of G. If the elements of G are represented as integers in the range $[0, |G| - 1]$ with addition in the group being integer addition modulo $|G|$, the discrete log problem is efficiently solved by an application of the extended Euclidean algorithm. However, there are representations of G in which the discrete log problem is thought to be hard in general. (Examples include realisations of G as a group of

points on an elliptic curve, or as a subgroup of the multiplicative group of a finite field.) Groups where the discrete log problem is hard are of great interest, since they can form the basis for key exchange protocols [4] and public key cryptosystems [5]. See Stinson [8] for a good introduction to the area.

Biggs [3] has recently proposed the critical group of a class of finite graphs as a candidate for a group with a hard discrete log problem. The purpose of this paper is to show that, in fact, these groups have an efficiently solvable discrete log problem and so are not suitable as platform groups for discrete log based cryptography.

In the next section, we will recap Biggs's construction of his class of critical groups. In the final section of the paper we will show, using the theory of Picard groups on finite graphs, that the discrete log problem can be efficiently solved.

2 A dollar-firing game on a graph

The abelian group that Biggs proposes as a platform for the discrete log problem is represented as a dollar-firing game on a graph. See Biggs [1, 2] for background on this area. We define the group as follows.

Let n be a positive integer (the security parameter of the problem). Let W be the wheel graph with $2n+1$ spokes. So W consists of a cycle $v_1, v_2, \ldots, v_{2n+1}$ (the 'rim' of the wheel) together with a 'hub' vertex q that is joined to each of the vertices v_i. Let $W^\dagger$ be the graph obtained from W by adding a vertex v_{2n+2} on the edge joining v_{2n+1} and v_1. We write V for the set of vertices of $W^\dagger$ and E for the set of edges of $W^\dagger$. We define $V^* = V \setminus \{q\}$, so V^* is the set of vertices on the rim of the modified wheel graph.

A *configuration* on $W^\dagger$ (with distinguished vertex q) is a function $s : V \to \mathbb{Z}$ such that $s(v) \geq 0$ for all $v \in V^*$ and such that $s(q) = -\sum_{v \in V^*} s(v)$. A *firing* of a vertex u is a move from a configuration s to a configuration s', where we reduce $s(u)$ by $\deg u$ and add 1 to each of the neighbours of u. So

$$s'(v) = \begin{cases} s(v) - \deg v & \text{if } v = u, \\ s(v) + 1 & \text{if } v \text{ and } u \text{ are adjacent,} \\ s(v) & \text{otherwise.} \end{cases}$$

A firing of a vertex u with $u \neq q$ is *legal* if $s(u) \geq \deg u$. A firing of q is *legal* if there are no legal firings of a vertex u with $u \neq q$. A configuration s is

stable if q is the only vertex that can be fired legally. A stable configuration s is *critical* if there is a non-empty sequence of legal firings that return to s. It is possible to show that given any starting configuration s, there is a unique critical configuration $\gamma(s)$ that can be reached by a sequence of legal firings starting at s.

The *critical group* $\mathcal{K}(W^\dagger)$ is the set of critical configurations, with addition of two configurations s and s' defined to be $\gamma(s + s')$. Note that an element of $\mathcal{K}(W^\dagger)$ may be specified by the vector $(s(u)_{u \in V^*})$ of length $2n+2$. Since $0 \leq s(u) \leq \deg u \leq 3$ for all $u \in V^*$, this representation is efficient. Moreover, a result of van den Heuvel [6] shows that a group operation can be computed using at most $O(n^3)$ firings, and so group operations may be carried out fairly efficiently.

Let f_n and ℓ_n be the nth Fibonacci and nth Lucas numbers respectively. Biggs [3] shows that $\mathcal{K}(W^\dagger)$ is cyclic of order τ, where $\tau = 2\ell_{2n+1}f_{2n+1}$.

3 A cryptanalysis using the Picard group

This section shows that the discrete log problem in $\mathcal{K}(W^\dagger)$ can be solved efficiently. We construct an isomorphism θ from $\mathcal{K}(W^\dagger)$ to the additive group $\mathbb{Z}/\tau\mathbb{Z}$ of integers modulo τ. Constructing the isomorphism is efficient, taking at most $O(n)$ integer operations and requiring the storage of $O(n)$ integers. Once this is done, an image under θ can be computed in $O(n)$ operations. Once θ has been constructed, we can solve the discrete log problem as follows. Given $g, h \in \mathcal{K}(W^\dagger)$ with h in the cyclic subgroup generated by g, we note that $\theta(h)$ lies in the subgroup generated by $\theta(g)$ and so we may find $k \in \mathbb{Z}$ such that $k\theta(g) = \theta(h)$ since the discrete log problem is easy in $\mathbb{Z}/\tau\mathbb{Z}$. But then k is a solution to our discrete log problem in $\mathcal{K}(W^\dagger)$, and we are done.

We construct θ as the composition of three isomorphisms ϕ, ψ and π, which we define below.

The *Picard group* $\mathrm{Pic}(W^\dagger)$ is an abelian group isomorphic to $\mathcal{K}(W^\dagger)$; see Biggs [1, Sections 28-32] for the relevant theory of this group. A concrete realisation of $\mathrm{Pic}(W^\dagger)$ is as follows. Let $\mathbb{Z}^{2n+2}$ be the free abelian group generated by V^*. Let Q' be the $(2n + 2) \times (2n + 2)$ matrix with rows and columns indexed by V^* where

$$Q'_{v_i v_j} = \begin{cases} \deg v_i & \text{if } i = j, \\ -1 & \text{if } i \neq j \text{ and } v_i \text{ and } v_j \text{ are adjacent,} \\ 0 & \text{otherwise.} \end{cases}$$

Then the Picard group is the quotient of $\mathbb{Z}^{2n+2}$ by the relations matrix Q'. (Let Q be the discrete Laplacian of $W^\dagger$. Then Q' is the result of removing the row and column indexed by the vertex q from Q, and so by [1, Proposition 30.1] this construction is indeed a realisation of $\mathrm{Pic}(W^\dagger)$.)

Let $\phi : \mathcal{K}(W^\dagger) \to \mathrm{Pic}(W^\dagger)$ take a critical configuration s to the obvious element of $\mathrm{Pic}(W^\dagger)$, namely the coset with representative $(s(u)_{u\in V^*})$. Then ϕ is an isomorphism [1, Proposition 32.2]. It is clearly trivial to compute the image of an element under ϕ.

Let A be the Smith Normal Form of the relations matrix Q' above. So

$$A = \mathrm{diag}(1, 1, \ldots, 1, 1, \tau),$$

since $\mathcal{K}(W^\dagger)$ is cyclic of order τ. Let $X, Y \in \mathrm{GL}(2n+2, \mathbb{Z})$ be such that $XQ'Y = A$. The matrices X and Y may be found by standard techniques using $O(n^3)$ integer operations. However, since Q' is of such a special form we can obtain the Smith Normal Form and the matrices X and Y much more efficiently. To see this, first note that replacing Q' by $-Q'$ and permuting its rows appropriately transforms Q' into the matrix Q'' where

$$Q'' = \begin{pmatrix} 1 & & & & & 1 & -2 \\ -3 & 1 & & & & & 1 \\ 1 & -3 & 1 & & & & \\ & \ddots & \ddots & \ddots & & & \\ & & 1 & -3 & 1 & & \\ & & & 1 & -3 & 1 & \\ & & & & 1 & -3 & 1 \end{pmatrix}.$$

But now it is easy to write down an explicit sequence of $O(n)$ elementary row operations that transforms Q'' into a matrix R of the form

$$R = \begin{pmatrix} I & M \\ 0 & N \end{pmatrix}$$

where I is the $2n \times 2n$ identity matrix, 0 is the $2 \times 2n$ all zero matrix and M and N are $2n \times 2$ and 2×2 integer matrices respectively. The matrices M and N contain $O(n)$ entries and can be efficiently computed from the last two columns of Q'' by tracing the effect of the sequence of row operations on these columns. Finding matrices $X', Y' \in \mathrm{GL}(2n+2, \mathbb{Z})$ such that $X'RY'$ is in Smith Normal Form now takes just $O(n)$ operations

(using standard algorithms), and since R is obtained from Q' using row operations alone we find that we may take $Y = Y'$. Note that Y is a sparse matrix, containing just $O(n)$ non-zero entries. Also note that we may work modulo τ to avoid problems with coefficients becoming too large: see for example Sims [7, Section 8.4].

Let G be the quotient of $\mathbb{Z}^{2n+2}$ by the relations matrix A. Define $\psi : \mathrm{Pic}(W^\dagger) \to G$ to be the map induced by right multiplication by Y. Then (see [7, Proposition 8.3.3]) ϕ is an isomorphism. Clearly ψ may be computed using $O(n)$ integer operations.

Finally, let $\pi : G \to \mathbb{Z}/\tau\mathbb{Z}$ be the map induced by projecting onto the last co-ordinate; once more it is clear that π is easy to compute.

If we define $\theta = \pi\psi\phi$, we have found an isomorphism with the properties we need; so the discrete log problem is efficiently solvable in $\mathcal{K}(W^\dagger)$ as claimed.

Acknowledgement The author would like to thank Steven Galbraith for his useful comments on an earlier draft of this paper.

References

[1] N.L. Biggs, 'Algebraic potential theory on graphs', *Bull. London Math. Soc.* 29 (1997) 641-682.

[2] N.L. Biggs, 'Chip-firing and the critical group of a graph', *J. Algebraic Combin.* 9 (1999) 25-45.

[3] N.L. Biggs, 'The critical group from a cryptographic perspective', *Bull. London Math. Soc.* 39 (2007) 829-836.

[4] W. Diffie and M.E. Hellman, 'New directions in cryptography', *IEEE Trans. Inform. Theory* 22 (1976), 644-654.

[5] T. ElGamal, 'A public key cryptosystem and a signature scheme based on discrete logarithms', *IEEE Trans. Inform. Theory* 31 (1985), 469-472.

[6] J. van den Heuvel, 'Algorithmic aspects of a chip-firing game', *Combin. Probab. Comput.* 10 (2001) 505-529.

[7] Charles C. Sims, *Computation with Finitely Presented Groups*, Cambridge University Press, UK, 1994.

[8] Douglas R. Stinson, *Cryptography: Theory and Practice* (2nd Edition) Chapman and Hall/CRC Press, Boca Raton, 2002.