Cryptanalysis of the Critical Group

Simon R. Blackburn

Royal Holloway, University of London

23rd October 2008

Overview

The discrete log problem

- Let G be an abelian group, written additively. Let $g \in G$.
- The discrete log problem for G: given some multiple h of g, find $k \in \mathbb{Z}$ such that $h = kg$.

The discrete log problem

- Let G be an abelian group, written additively. Let $g \in G$.
- The discrete log problem for G: given some multiple h of g, find $k \in \mathbb{Z}$ such that $h = kg$.
- There should be a concrete way of writing down the elements of G.

The discrete log problem

- Let G be an abelian group, written additively. Let $g \in G$.
- The discrete log problem for G: given some multiple h of g, find $k \in \mathbb{Z}$ such that $h = kg$.
- There should be a concrete way of writing down the elements of G.
- The discrete log problem should be difficult.

The discrete log problem

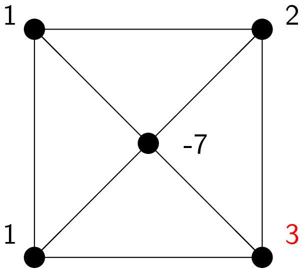
- Let G be an abelian group, written additively. Let $g \in G$.
- The discrete log problem for G: given some multiple h of g, find $k \in \mathbb{Z}$ such that $h = kg$.
- There should be a concrete way of writing down the elements of G.
- The discrete log problem should be difficult.
- G is known as a platform group.

A dollar-firing game

Let $\Gamma = (V, E)$ be a graph. Let $q \in V$ be a vertex.
A configuration: a function $s : V \to \mathbb{Z}$ such that $s(v) \geq 0$ for $v \neq q$, and $\sum_v s(v) = 0$.
A firing: for a fixed $u \in V$, move a dollar along every edge away from u.

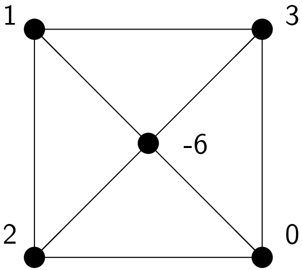
A dollar-firing game

Let $\Gamma = (V, E)$ be a graph. Let $q \in V$ be a vertex.
A configuration: a function $s : V \to \mathbb{Z}$ such that $s(v) \geq 0$ for $v \neq q$, and $\sum_v s(v) = 0$.
A firing: for a fixed $u \in V$, move a dollar along every edge away from u.



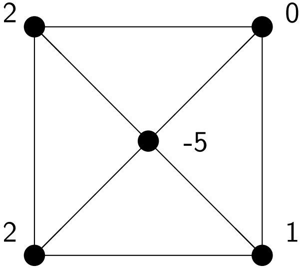
A dollar-firing game

Let $\Gamma = (V, E)$ be a graph. Let $q \in V$ be a vertex.
A configuration: a function $s : V \to \mathbb{Z}$ such that $s(v) \geq 0$ for $v \neq q$, and $\sum_v s(v) = 0$.
A firing: for a fixed $u \in V$, move a dollar along every edge away from u.



A dollar-firing game

Let $\Gamma = (V, E)$ be a graph. Let $q \in V$ be a vertex.
A configuration: a function $s : V \to \mathbb{Z}$ such that $s(v) \geq 0$ for $v \neq q$, and $\sum_v s(v) = 0$.
A firing: for a fixed $u \in V$, move a dollar along every edge away from u.



Critical configurations

A firing with $u \neq q$ is legal if $s(u) \geq \deg u$.
A firing with $u = q$ is legal if there are no other legal firings.

Critical configurations

A firing with $u \neq q$ is legal if $s(u) \geq \deg u$.

A firing with $u = q$ is legal if there are no other legal firings.

A stable configuration: q is the only vertex that can be fired legally.

A critical configuration s: stable and $\exists$ a sequence of legal firings that return to s.

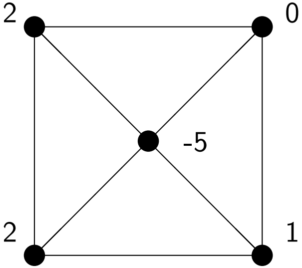
Critical configurations

A firing with $u \neq q$ is legal if $s(u) \geq \deg u$.

A firing with $u = q$ is legal if there are no other legal firings.

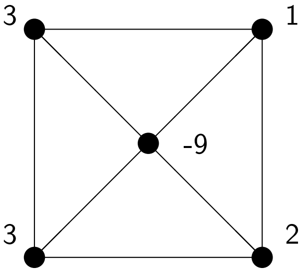
A stable configuration: q is the only vertex that can be fired legally.

A critical configuration s: stable and $\exists$ a sequence of legal firings that return to s.



Critical configurations

A firing with $u \neq q$ is legal if $s(u) \geq \deg u$.
A firing with $u = q$ is legal if there are no other legal firings.
A stable configuration: q is the only vertex that can be fired legally.
A critical configuration s: stable and $\exists$ a sequence of legal firings that return to s.



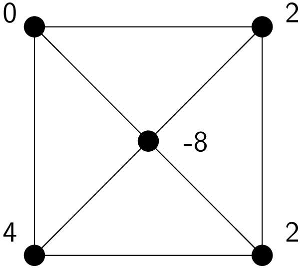
Critical configurations

A firing with $u \neq q$ is legal if $s(u) \geq \deg u$.

A firing with $u = q$ is legal if there are no other legal firings.

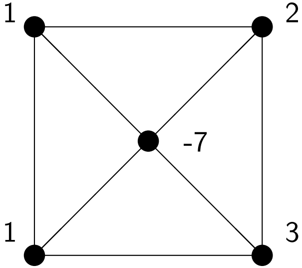
A stable configuration: q is the only vertex that can be fired legally.

A critical configuration s: stable and $\exists$ a sequence of legal firings that return to s.



Critical configurations

A firing with $u \neq q$ is legal if $s(u) \geq \deg u$.
A firing with $u = q$ is legal if there are no other legal firings.
A stable configuration: q is the only vertex that can be fired legally.
A critical configuration s: stable and $\exists$ a sequence of legal firings that return to s.



The critical group

$\gamma(s)$: the unique critical configuration reached by legal firings starting at s.

The critical group

$\gamma(s)$: the unique critical configuration reached by legal firings starting at s.

Definition

The critical group $\mathcal{K}(\Gamma)$ is the set of critical configurations, with addition of s and s' defined to be $\gamma(s+s')$.

The critical group

$\gamma(s)$: the unique critical configuration reached by legal firings starting at s.

Definition

The critical group $\mathcal{K}(\Gamma)$ is the set of critical configurations, with addition of s and s' defined to be $\gamma(s + s')$.

- The critical group of a finite connected graph Γ does not depend on q.

The critical group

$\gamma(s)$: the unique critical configuration reached by legal firings starting at s.

Definition

The critical group $\mathcal{K}(\Gamma)$ is the set of critical configurations, with addition of s and s' defined to be $\gamma(s+s')$.

- The critical group of a finite connected graph Γ does not depend on q.
- The critical group is finite and abelian.

The critical group

$\gamma(s)$: the unique critical configuration reached by legal firings starting at s.

Definition

The critical group $\mathcal{K}(\Gamma)$ is the set of critical configurations, with addition of s and s' defined to be $\gamma(s+s')$.

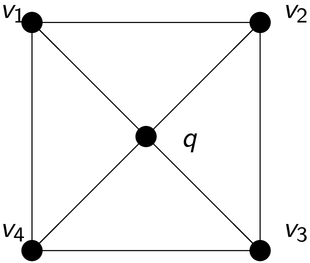
- The critical group of a finite connected graph Γ does not depend on q.
- The critical group is finite and abelian.
- Addition may be carried out using at most $O(|V|^3)$ firings. [van den Heuvel, *Combin. Probab. Comput.* 2001]

The proposed platform group

Take the wheel graph with vertices $v_1, v_2, \ldots, v_{2n+2}$ on the 'rim', and a 'hub' vertex q.
Remove the spoke at v_{2n+2}, to obtain a graph $W^\dagger$.

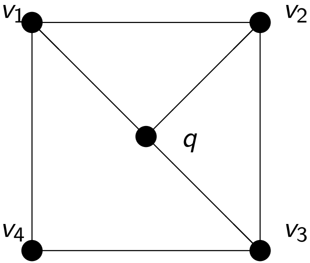
The proposed platform group

Take the wheel graph with vertices $v_1, v_2, \ldots, v_{2n+2}$ on the 'rim', and a 'hub' vertex q.
Remove the spoke at v_{2n+2}, to obtain a graph $W^\dagger$.



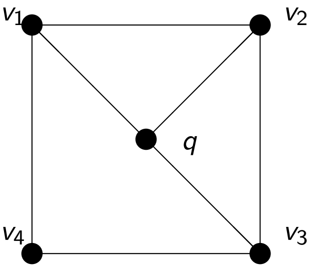
The proposed platform group

Take the wheel graph with vertices $v_1, v_2, \ldots, v_{2n+2}$ on the 'rim', and a 'hub' vertex q.
Remove the spoke at v_{2n+2}, to obtain a graph $W^\dagger$.



The proposed platform group

Take the wheel graph with vertices $v_1, v_2, \ldots, v_{2n+2}$ on the 'rim', and a 'hub' vertex q.
Remove the spoke at v_{2n+2}, to obtain a graph $W^\dagger$.



Proposed as a platform group by [Biggs, *Bull. LMS.* 2007]

Advantages of $\mathcal{K}(W^{\dagger})$

- Cyclic.
- Concrete representation of elements: $O(n)$ bits.
- Efficient addition: $O(n^3)$ operations.
- Exponential order: $2\ell_{2n+1}f_{2n+2}$ elements.

Advantages of $\mathcal{K}(W^\dagger)$

- Cyclic.
- Concrete representation of elements: $O(n)$ bits.
- Efficient addition: $O(n^3)$ operations.
- Exponential order: $2\ell_{2n+1}f_{2n+2}$ elements.

Question: Is the discrete log problem hard?

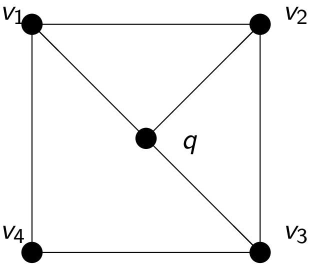
Advantages of $\mathcal{K}(W^\dagger)$

- Cyclic.
- Concrete representation of elements: $O(n)$ bits.
- Efficient addition: $O(n^3)$ operations.
- Exponential order: $2\ell_{2n+1}f_{2n+2}$ elements.

Question: Is the discrete log problem hard?

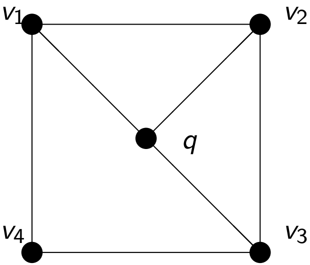
Answer: No.

Another perspective on $\mathcal{K}(W^\dagger)$:



'Configurations': $s_1 v_1 + s_2 v_2 + s_3 v_3 + s_4 v_4$ where $s_i \in \mathbb{Z}$ (free abelian group of rank $|V| - 1 = 4$).

Another perspective on $\mathcal{K}(W^\dagger)$:



'Configurations': $s_1 v_1 + s_2 v_2 + s_3 v_3 + s_4 v_4$ where $s_i \in \mathbb{Z}$ (free abelian group of rank $|V| - 1 = 4$).
Firings: $|V|$ relations.

$$\begin{array}{ll} 3v_1 = v_2 + v_4 & 3v_2 = v_1 + v_3 \\ 3v_3 = v_2 + v_4 & 2v_4 = v_1 + v_3 \end{array}$$

plus the dependent relation $0 = v_1 + v_2 + v_3$.

The Picard group

Definition

The Picard group $\mathrm{Pic}(\Gamma)$ is constructed as follows. Take the free abelian group generated by $|V| - 1$ elements $v \in V \setminus \{q\}$. Add a corresponding relation for each firing at a vertex $u \neq q$.

The Picard group

Definition

The Picard group $\mathrm{Pic}(\Gamma)$ is constructed as follows. Take the free abelian group generated by $|V|-1$ elements $v \in V \setminus \{q\}$. Add a corresponding relation for each firing at a vertex $u \neq q$.

Theorem

For any connected graph Γ, $\mathrm{Pic}(\Gamma) \cong \mathcal{K}(\Gamma)$.

(See Biggs, *Bull. LMS*, 1997)

The relations of $\mathrm{Pic}(W^\dagger)$

The relations matrix of the Picard group of $W^\dagger$:

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

A cryptanalysis

- Compute the Smith Normal Form A of the relations matrix Q'':
$$XQ''Y = A \text{ where } X, Y \in \mathrm{GL}(2n+2, \mathbb{Z}).$$

A cryptanalysis

- Compute the Smith Normal Form A of the relations matrix Q'':

$$XQ''Y = A \text{ where } X, Y \in \mathrm{GL}(2n+2, \mathbb{Z}).$$

- Biggs tells us $\mathcal{K}(W^\dagger)$ is cyclic, so

$$A = \mathrm{diag}(1, 1, 1, \ldots, 1, |\mathcal{K}(W^\dagger)|).$$

A cryptanalysis

- Compute the Smith Normal Form A of the relations matrix Q'':
$$XQ''Y = A \text{ where } X, Y \in \mathrm{GL}(2n+2, \mathbb{Z}).$$
- Biggs tells us $\mathcal{K}(W^\dagger)$ is cyclic, so
$$A = \mathrm{diag}(1, 1, 1, \ldots, 1, |\mathcal{K}(W^\dagger)|).$$
- Let G be the quotient of $\mathbb{Z}^{2n+2}$ by the relations A. Then $\mathcal{K}(W^\dagger) \cong G$, via the map
$$\mathbf{s} \mapsto \mathbf{s}X.$$

A cryptanalysis

- Compute the Smith Normal Form A of the relations matrix Q'':
$$XQ''Y = A \text{ where } X, Y \in \mathrm{GL}(2n+2, \mathbb{Z}).$$

- Biggs tells us $\mathcal{K}(W^\dagger)$ is cyclic, so
$$A = \mathrm{diag}(1, 1, 1, \ldots, 1, |\mathcal{K}(W^\dagger)|).$$

- Let G be the quotient of $\mathbb{Z}^{2n+2}$ by the relations A. Then $\mathcal{K}(W^\dagger) \cong G$, via the map
$$\mathbf{s} \mapsto \mathbf{s}X.$$

- The discrete log problem in G is trivial to solve.

Conclusion

- Bigg's cryptosystem is insecure: a SNF computation of $O(n^3)$ integer operations is the main cryptanalytic cost.

Conclusion

- Bigg's cryptosystem is insecure: a SNF computation of $O(n^3)$ integer operations is the main cryptanalytic cost.
- The special structure of Q'' can be used to reduce the complexity of the attack to $O(n)$ integer operations.

Conclusion

- Bigg's cryptosystem is insecure: a SNF computation of $O(n^3)$ integer operations is the main cryptanalytic cost.
- The special structure of Q'' can be used to reduce the complexity of the attack to $O(n)$ integer operations.
- The $O(n^3)$ attack applies to any graph, not just $W^\dagger$.

Some Links

This talk will appear soon on my home page:

`http://www.cs.rhbnc.ac.uk/~simonb/`

The paper 'Cryptanalysing the critical group' is available at:

`http://eprint.iacr.org/2008/170`