Group Theory and Cryptography

Simon R. Blackburn

Royal Holloway, University of London

14th August 2009

Overview

Discrete logarithm problem (DLP)

Let p be a prime and let $g, h \in \mathbb{Z}_p^*$.
Find an integer x (if it exists) such that $h \equiv g^x \mod p$.

Discrete logarithm problem (DLP)

Let p be a prime and let $g, h \in \mathbb{Z}_p^*$.
Find an integer x (if it exists) such that $h \equiv g^x \mod p$.

In general, this is a hard computational problem (for large p).

Example: Let $p = 11$, $g = 2$ and $h = 9$. Solve the DLP.

Discrete logarithm problem (DLP)

Let p be a prime and let $g, h \in \mathbb{Z}_p^*$.
Find an integer x (if it exists) such that $h \equiv g^x \mod p$.

In general, this is a hard computational problem (for large p).

Example: Let $p = 11$, $g = 2$ and $h = 9$. Solve the DLP.

x	0	1	2	3	4	5	6	7	8	9
g^x	1	2	4	8	5	10	9	7	3	6

Diffie-Hellman key exchange

Suppose Alice and Bob want to agree on a random key K.
They decide upon a large prime p and some $g \in \mathbb{Z}_p^*$ and perform the following protocol:

Diffie-Hellman key exchange

Suppose Alice and Bob want to agree on a random key K.
They decide upon a large prime p and some $g \in \mathbb{Z}_p^*$ and perform the following protocol:

- Alice chooses a random integer $1 \leq a < p-1$ and sends $c_1 = g^a \mod p$ to Bob.

Diffie-Hellman key exchange

Suppose Alice and Bob want to agree on a random key K.
They decide upon a large prime p and some $g \in \mathbb{Z}_p^*$ and perform the following protocol:

- Alice chooses a random integer $1 \leq a < p-1$ and sends $c_1 = g^a \mod p$ to Bob.
- Bob chooses a random integer $1 \leq b < p-1$ and sends $c_2 = g^b \mod p$ to Alice.

Diffie-Hellman key exchange

Suppose Alice and Bob want to agree on a random key K.
They decide upon a large prime p and some $g \in \mathbb{Z}_p^*$ and perform the following protocol:

- Alice chooses a random integer $1 \leq a < p-1$ and sends $c_1 = g^a \mod p$ to Bob.
- Bob chooses a random integer $1 \leq b < p-1$ and sends $c_2 = g^b \mod p$ to Alice.

Alice and Bob both share the same key $K = g^{ab} \mod p$.

Diffie-Hellman key exchange

Suppose Alice and Bob want to agree on a random key K.
They decide upon a large prime p and some $g \in \mathbb{Z}_p^*$ and perform the following protocol:

- Alice chooses a random integer $1 \leq a < p-1$ and sends $c_1 = g^a \mod p$ to Bob.
- Bob chooses a random integer $1 \leq b < p-1$ and sends $c_2 = g^b \mod p$ to Alice.
- On receiving c_2 Alice computes $K = c_2^a \mod p$.

Alice and Bob both share the same key $K = g^{ab} \mod p$.

Diffie-Hellman key exchange

Suppose Alice and Bob want to agree on a random key K.
They decide upon a large prime p and some $g \in \mathbb{Z}_p^*$ and perform the following protocol:

- Alice chooses a random integer $1 \leq a < p-1$ and sends $c_1 = g^a \mod p$ to Bob.
- Bob chooses a random integer $1 \leq b < p-1$ and sends $c_2 = g^b \mod p$ to Alice.
- On receiving c_2 Alice computes $K = c_2^a \mod p$.
- On receiving c_1 Bob computes $K = c_1^b \mod p$.

Alice and Bob both share the same key $K = g^{ab} \mod p$.

Diffie-Hellman key exchange

Suppose Alice and Bob want to agree on a random key K.
They decide upon a large prime p and some $g \in \mathbb{Z}_p^*$ and perform the following protocol:

- Alice chooses a random integer $1 \leq a < p-1$ and sends $c_1 = g^a \mod p$ to Bob.
- Bob chooses a random integer $1 \leq b < p-1$ and sends $c_2 = g^b \mod p$ to Alice.
- On receiving c_2 Alice computes $K = c_2^a \mod p$.
- On receiving c_1 Bob computes $K = c_1^b \mod p$.

Alice and Bob both share the same key $K = g^{ab} \mod p$.

Alice and Bob have the same key: $(g^a)^b = (g^b)^a$.

How hard is the DLP?

- The DLP in $\mathbb{Z}_p^*$ is thought to be hard, but there are subexponential algorithms to solve it.

How hard is the DLP?

- The DLP in $\mathbb{Z}_p^*$ is thought to be hard, but there are subexponential algorithms to solve it.
- The DLP makes sense for any cyclic group.

How hard is the DLP?

- The DLP in $\mathbb{Z}_p^*$ is thought to be hard, but there are subexponential algorithms to solve it.
- The DLP makes sense for any cyclic group.
- The group of points on an elliptic curve is thought to be more secure.

How hard is the DLP?

- The DLP in $\mathbb{Z}_p^*$ is thought to be hard, but there are subexponential algorithms to solve it.
- The DLP makes sense for any cyclic group.
- The group of points on an elliptic curve is thought to be more secure.
- Are there other good examples?

How hard is the DLP?

- The DLP in $\mathbb{Z}_p^*$ is thought to be hard, but there are subexponential algorithms to solve it.
- The DLP makes sense for any cyclic group.
- The group of points on an elliptic curve is thought to be more secure.
- Are there other good examples?
- Note: Integers mod n under addition is a bad choice.

How hard is the DLP?

- The DLP in $\mathbb{Z}_p^*$ is thought to be hard, but there are subexponential algorithms to solve it.
- The DLP makes sense for any cyclic group.
- The group of points on an elliptic curve is thought to be more secure.
- Are there other good examples?
- Note: Integers mod n under addition is a bad choice.
- What about non-abelian groups?

Ko Lee Cheon Han Kang Park

- Let G be a (non-abelian) group. For $a, g \in G$ define

$$g^a = a^{-1}ga.$$

Ko Lee Cheon Han Kang Park

- Let G be a (non-abelian) group. For $a, g \in G$ define

$$g^a = a^{-1}ga.$$

- Problem: $(g^a)^b \neq (g^b)^a$, in general.

Ko Lee Cheon Han Kang Park

- Let G be a (non-abelian) group. For $a, g \in G$ define

$$g^a = a^{-1}ga.$$

- Problem: $(g^a)^b \neq (g^b)^a$, in general.
- Solution: Choose $a \in A \leq G$ and $b \in B \leq G$ where $[A, B] = \{1\}$.

Ko Lee Cheon Han Kang Park

- Let G be a (non-abelian) group. For $a, g \in G$ define

$$g^a = a^{-1}ga.$$

- Problem: $(g^a)^b \neq (g^b)^a$, in general.
- Solution: Choose $a \in A \leq G$ and $b \in B \leq G$ where $[A, B] = \{1\}$.
- How do you choose a group G and subgroups A and B?

Ko Lee Cheon Han Kang Park

- Let G be a (non-abelian) group. For $a, g \in G$ define

$$g^a = a^{-1}ga.$$

- Problem: $(g^a)^b \neq (g^b)^a$, in general.
- Solution: Choose $a \in A \leq G$ and $b \in B \leq G$ where $[A, B] = \{1\}$.
- How do you choose a group G and subgroups A and B?
- Ko et al. suggest using a braid group.

Braid group cryptography

- How difficult is the *conjugacy search problem*?
- There's a nice survey: 'Braid based cryptography' by Patrick Dehornoy.

Braid group cryptography

- How difficult is the *conjugacy search problem*?
- There's a nice survey: 'Braid based cryptography' by Patrick Dehornoy.
- Length based attacks work for many instances.

Braid group cryptography

- How difficult is the *conjugacy search problem*?
- There's a nice survey: 'Braid based cryptography' by Patrick Dehornoy.
- Length based attacks work for many instances.
- How can we generate hard instances?

Braid group cryptography

- How difficult is the *conjugacy search problem*?
- There's a nice survey: 'Braid based cryptography' by Patrick Dehornoy.
- Length based attacks work for many instances.
- How can we generate hard instances?
- There are no secure and practical braid based schemes known.

Other ideas

- Logarithmic signatures are another way to generalise the DLP.
- There is a nice idea due to Anshel, Anshel and Goldfeld.

Other ideas

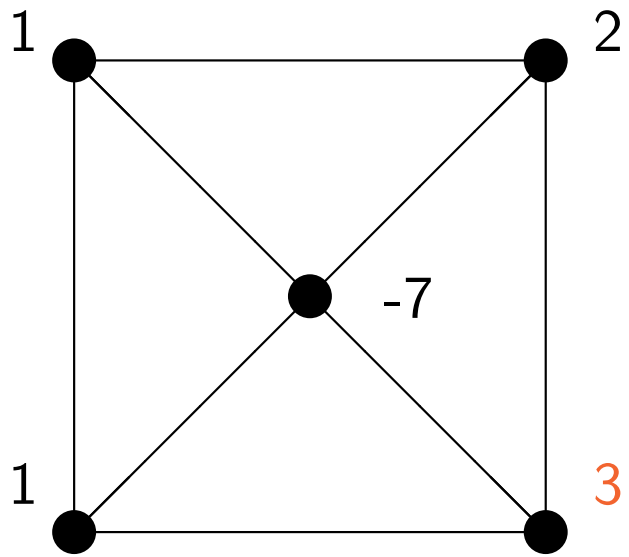
- Logarithmic signatures are another way to generalise the DLP.
- There is a nice idea due to Anshel, Anshel and Goldfeld.
- There are no group-based cryptosystems that have stood up to long term scrutiny.
- Other *Post-Quantum* cryptosystems might have more potential.
- Let's turn to the cryptanalysis of a specific proposal.

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.

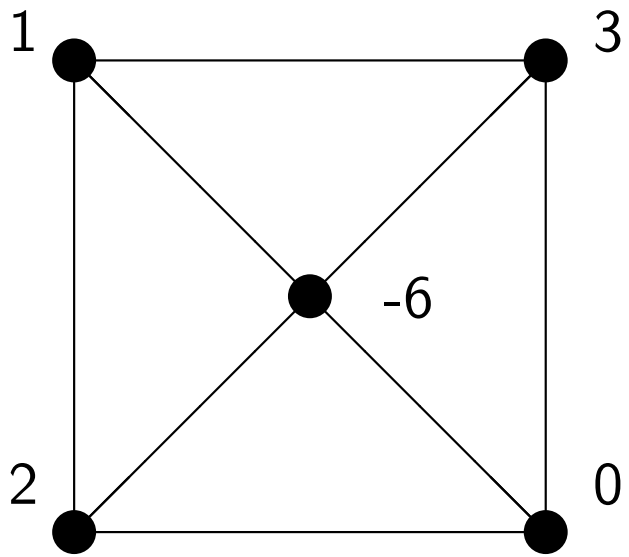
A dollar-firing game

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.



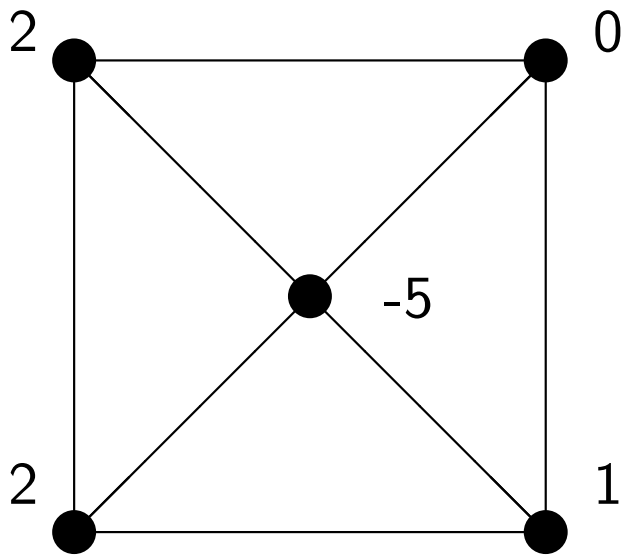
A dollar-firing game

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

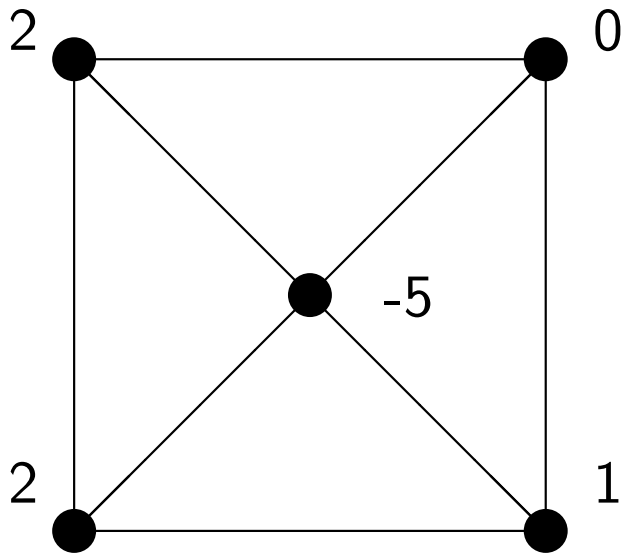
A firing with $u \neq q$ is legal if $s(u) \geq \deg u$.
A firing with $u = q$ is legal if there are no other legal firings.

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 returns to s.

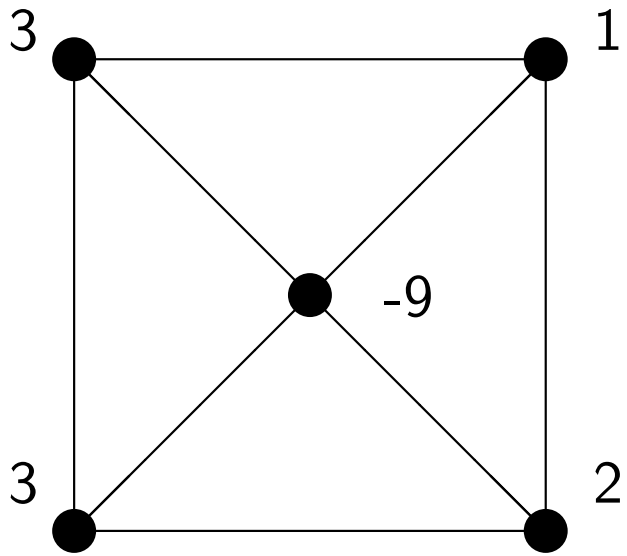
Critical configurations

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 returns to s.



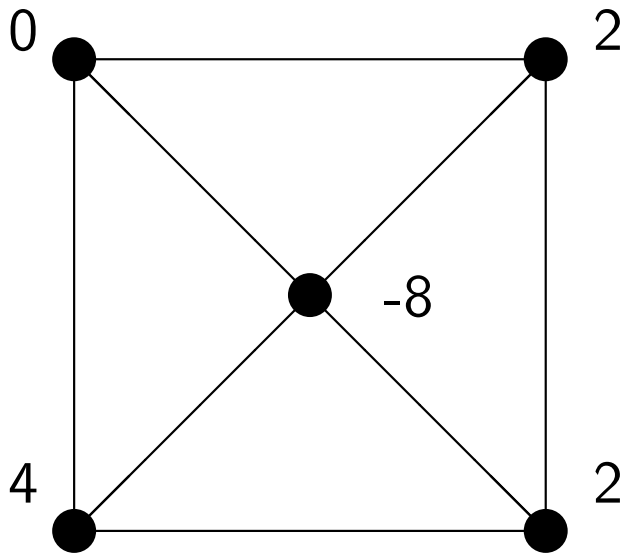
Critical configurations

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 returns to s.



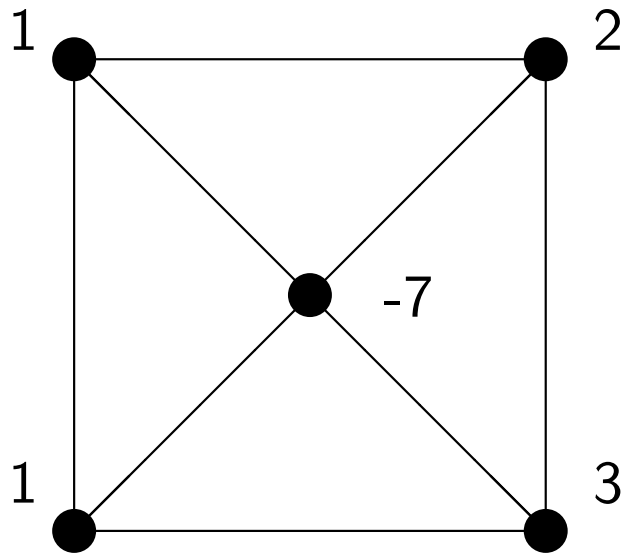
Critical configurations

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 returns 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 returns 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 $\gamma(s + s')$.

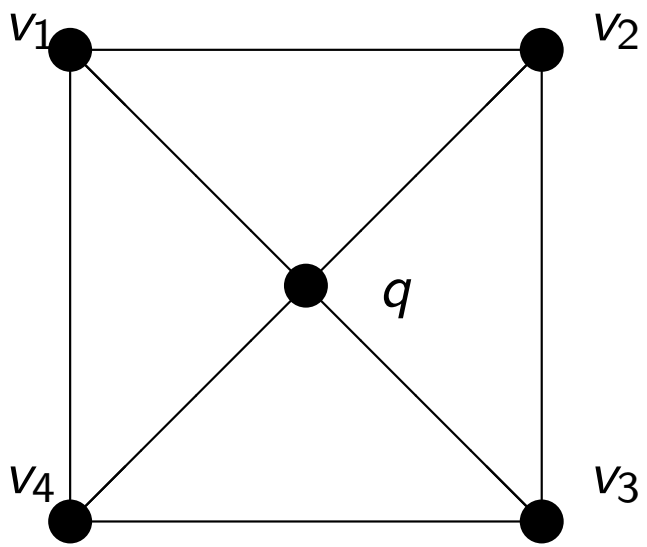
- The critical group of a finite connected graph Γ does not depend on q.
- The critical group is finite and abelian.
- Addition may be carried out using at most $O(|V|^3)$ firings. [van den Heuvel, *Combin. Probab. Comput.* 2001]

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 $W^\dagger$.

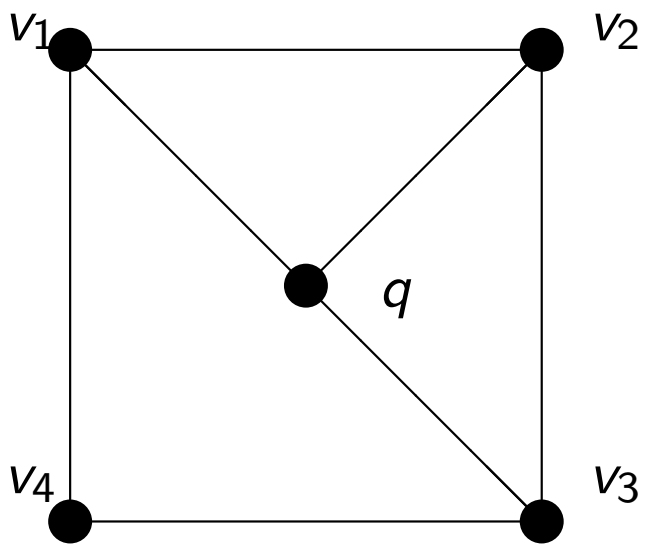
The proposed platform group

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 $W^\dagger$.



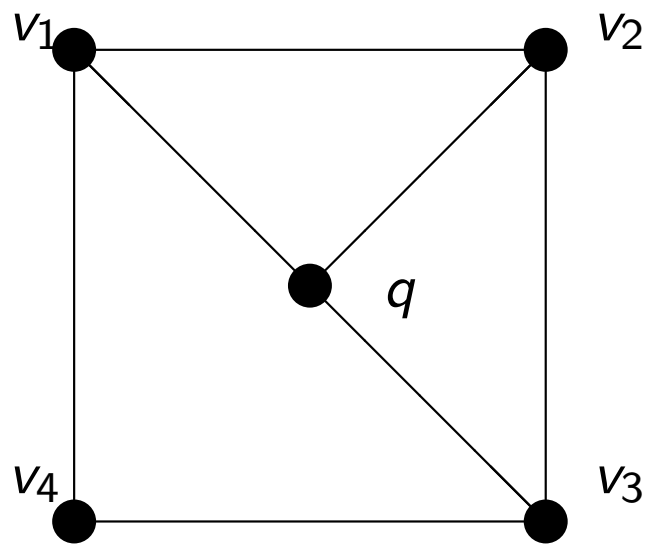
The proposed platform group

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?

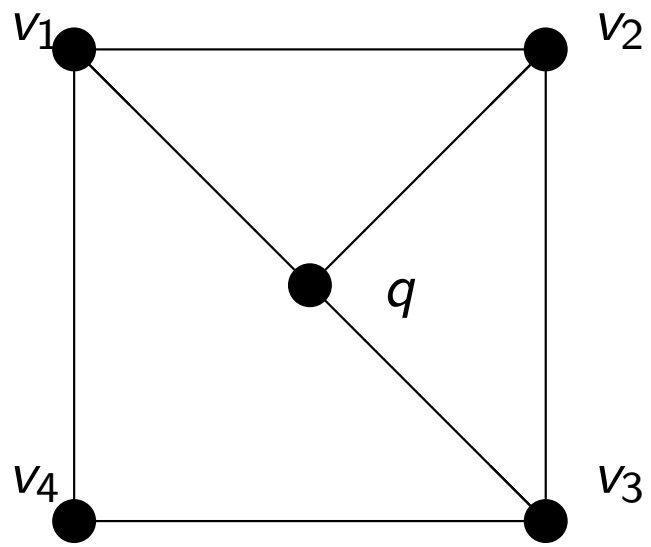
Advantages of $\mathcal{K}(W^\dagger)$

- 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?

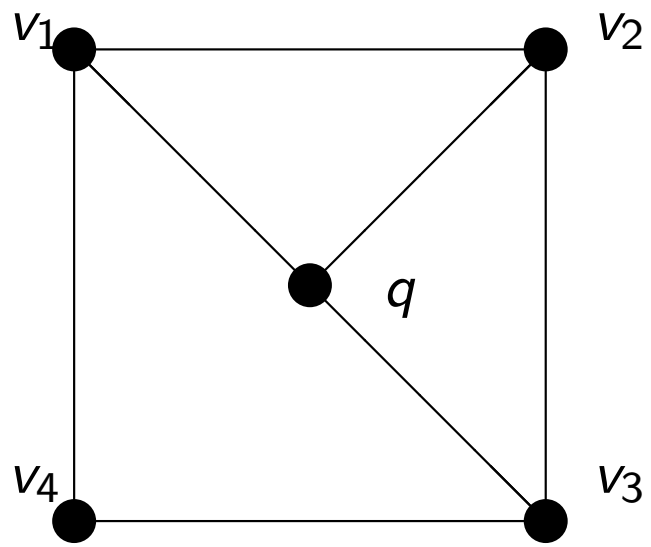
Answer: No.

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.

$$3v_1 = v_2 + v_4 \quad 3v_2 = v_1 + v_3$$
$$3v_3 = v_2 + v_4 \quad 2v_4 = v_1 + v_3$$

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

- Biggs' cryptosystem is insecure: a SNF computation is the main cryptanalytic cost.

Conclusion

- Biggs' cryptosystem is insecure: a SNF computation 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

- Biggs' cryptosystem is insecure: a SNF computation 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 SNF attack applies to any graph, not just $W^{\dagger}$.

Some Links

This talk will appear soon on my home page:

`http://www.ma.rhul.ac.uk/sblackburn`

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

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

Some Links

This talk will appear soon on my home page:

`http://www.ma.rhul.ac.uk/sblackburn`

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

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

S.R. Blackburn, C. Cid, C. Mullan, 'Group theory in cryptography' is available at:

`http://arxiv.org/abs/0906.5545`