Asymptotic algebra and modern cryptanalysis

Alexei Myasnikov

McGill University (Montreal)
Algebraic Cryptography Center (Stevens Inst.)
Search for generically hard problems

Plan:

- Generic Properties of van Kampen diagrams
- Asymptotically dominant subgroups
- Cryptanalysis of group based cryptosystems
Generic properties of van Kampen diagrams.

Let $X$ be a finite set (generators), $R$ a finite set of words in the alphabet $(X \cup X^{-1})^*$ (relators),

$$P = \langle X; R \rangle$$ a finite presentation (of a group $G$).

$\mathcal{D}(P)$ - the set of all van Kampen diagrams over $P$ equipped with the measure constructed above.

Our goal: to study generic properties of van Kampen diagrams over $P$.

A property $\mathcal{C}$ is generic if the set $\mathcal{D}_C$ of van Kampen diagrams satisfying $\mathcal{C}$ is generic in $\mathcal{D}(P)$. 
Linear isoperimetric inequalities and hyperbolicity

A van Kampen diagram $D$ over $P$ satisfies the linear isoperimetric inequality with coefficient $c$ if

$$\text{Area}(D) \leq c \text{L}(D)$$

where $\text{area}(D)$ is the area of $D$ and $L(D)$ is the length of the boundary (perimeter) of $D$.

**Gromov:** A group $G$ given by a finite presentation $P$ is hyperbolic if and only if there exists a constant $c$ such that every reduced van Kampen diagram over $P$ satisfies the linear isoperimetric inequality with the coefficient $c$. 
Generic hyperbolicity

Theorem [M.-Ushakov] The set of all van Kampen diagrams satisfying the linear isoperimetric inequality with coefficient 4

$$\text{area}(D) \leq 4L(D)$$

is strongly generic in $\mathcal{D}(P)$. 
Global and local generic hyperbolicity

**Generic Global Hyperbolicity [Gromov]:** A generic finitely presented group is hyperbolic.

**Generic Local Hyperbolicity [M.-Ushakov]:** Every finitely presented group is generically hyperbolic.
Generic depth of van Kampen diagrams.

**Theorem [M.-Ushakov]** The set of all van Kampen diagrams satisfying the logarithmic depth-area inequality

\[ \text{Depth}(D) \leq \log \text{Area}(D) \]

is generic in \( \mathcal{D}(P) \).

**Corollary.** The set of all van Kampen diagrams satisfying the logarithmic depth-perimeter inequality

\[ \text{Depth}(D) \leq \log L(D) + \log 4 \]

is generic in \( \mathcal{D}(P) \).
Generic complexity of the word problem

Theorem [M.-Ushakov] For a given finitely presented group $G = \langle X; R \rangle$ the algorithm $A_W$ solves the Search Word Problem in $G$ generically in polynomial time.

Indeed, recall the complexity of the algorithm $A_W$:

$$O(|w|L(R)^{Depth(w)})$$

where $L(R)$ is the total length of the presentation of $G$, and $Depth(w)$ is the minimal depth of van Kampen diagrams presenting $w$. 
Structure of a random van Kampen diagram.
Asymptotically dominant subgroups and Cryptanalysis
Anshel-Anshel-Goldfeld scheme

Public: Group $G$ with two f.g. subgroups

$A = \langle a_1, \ldots, a_m \rangle$, $B = \langle b_1, \ldots, b_n \rangle$

Alice: takes a (secret) word $a = u(a_1, \ldots, a_m)$ in alphabet $A^{\pm 1}$, encodes (by normal forms), and makes public:

$b_1^a, \ldots, b_n^a$

Bob: takes a (secret) word $b = v(b_1, \ldots, b_n)$ in alphabet $B^{\pm 1}$, encodes (by normal forms), and makes public:

$a_1^b, \ldots, a_m^b$

Shared secret key: $a^{-1}a^b = [a, b] = (b^a)^{-1}b$
Attacks on AAG schemes

- Conjugacy problem
- Normal forms
- Subgroups
Search for the Platform $G$

Known platforms:

- Braid groups,
- Thompson groups,
- Miller groups,
- Polycyclic groups,
- Free metabelian groups.
Naive attempts

Attempt 1:

$G = F(A)$ - free group on $A = \{a_1, \ldots, a_n\}$. 
The Conjugacy Problem in free groups

$u^x = v$ in $F(A)$:

Algorithm:

- find $\tilde{u}$ of minimal length among all conjugates of $u$,
- find $\tilde{v}$ of minimal length among all conjugates of $v$,
- $u^x = v \iff \tilde{v}$ is a cyclic permutation of $\tilde{u}$ and $x$ is an initial segment of $\tilde{u}$. 
Conjugacy Game (length based attack):

**Player 1:** for a given \( u \) has to find \( \tilde{u} \). The word \( u \) is not known to him but he may ask questions about the length of elements.

**Player 2:** does the required manipulations and tells the length of the resulting words

**Winning strategy** for Player 1:

- find \( b_1 \in A^{\pm 1} \) such that \( l(u^{b_1}) < l(u) \)

- repeat for \( u_1 = u^{b_1} \)

- output \( x = b_1 \ldots b_k \)
Whitehead-type attacks on CP

$u^x = v$ in a group $G$:

- find "minimal length" elements $\tilde{u}$, $\tilde{v}$ in the conjugacy classes of $u$ and $v$

- solve CP for $\tilde{u}$, $\tilde{v}$ (typically the conjugator is short)
Naive Search for the Platform

Attempt 2: $G = F(A)$ - free group on $A$ as before.

But $G$ is given by a finite non-standard presentation:

$$G = \langle X; R \rangle$$

The Length-Based Attack will work if we can compute the length of elements in $G$ relative to the standard presentation $G' = \langle A; \emptyset \rangle$
Geodesic length of elements

Let $G = \langle X; R \rangle$

$w$ is an element of $G$ given as a word in $X \cup X^{-1}$

The geodesic length $L(w)$ of $w$ is the length of a minimal path from 1 to $w$ in the Cayley graph of $G$ (with respect to the generating set $X$).

$$L(w) = \min \{|u| \mid u =_{G} w\}$$

The Word Problem is decidable in $G \iff$ the function $L : w \rightarrow L(w)$ is computable.
The geodesic length problem

**Geodesic Length Problem:** Given $G = \langle X; R \rangle$ and a word $w$ in $X \cup X^{-1}$ compute the geodesic length $l(w)$ of the element $w$.

If $G$ has undecidable word problem?

Compute the length on a generic subset.

Moreover, compute the length approximately.
Cryptanalysis of Attempt 2

**Attempt 2:** $G = F(A)$ is a free group on $A$ given by a finite non-standard presentation:

$$G = \langle X; R \rangle$$

The length-Based Attack works if one can "compute" the geodesic length function $L(w)$. 
**Known Platforms: Braid Groups**

\[ B_n - \text{the group of } n\text{-string braids.} \]

Classical Artin presentation:

\[ B_n = \langle x_1, \ldots, x_{n-1} \mid x_ix_{i+1}x_i = x_{i+1}x_ix_{i+1}, \quad 1 \leq i \leq n-2 \\
\quad x_ix_j = x_jx_i, \quad |i-j| > 1, \quad 1 \leq i, j \leq n-1 \rangle \]
Normal Forms in Braid Groups

Garside normal forms:

Time complexity to compute the normal form of \( b \in B_n \) is bounded by \( O(|b|^{2n \log n}) \).

Dehornoy normal forms:

Time complexity: not known (believed to be "fast" on most inputs)
Conjugacy Problem

• CP is decidable, but the time complexity is not known

• Not known to be of polynomial time.

• Known to be of polynomial time on ”most” inputs
Subgroup attacks

Main ideas:

- "Random" subgroups of a given group are "very particular"
- CP is very particular in random subgroups
- Length base attacks
Random Subgroups

Let $G$ be a group with a finite set of generators $X$.

**Main Question:** What are random subgroups in $G$?

No subgroup Cayley Graphs, no random walks on them.
Random Generator of subgroups in $G$:

- pick a random $k \in \mathbb{N}$

- pick randomly $k$ words $w_1, \ldots, w_k \in F(X)$

- generate a subgroup $\langle w_1, \ldots, w_k \rangle$ of $G$. 
Asymptotically visible subgroups

Fix $k \in \mathbb{N}$. For $t \in \mathbb{N}$ put

$$Sub_t(X, k) = \{(w_1, \ldots, w_k) \mid w_i \in F(X), |w_i| \leq t\}$$

For a group $H$ put

$$Sub_t(G, X, H, k) = \{(w_1, \ldots, w_k) \in Sub_t(X, k) \mid \langle w_1, \ldots, w_k \rangle \simeq H\}$$

Then the ratio

$$f_t(G, X, H, k) = \frac{|Sub_t(G, X, H, k)|}{|Sub_t(X, k)|}$$

gives the frequency of subgroups isomorphic to $H$ that occur among all subgroups generated by $k$-tuples of words in $X^{\pm 1}$ of length at most $t$. 
$H$ is **asymptotically dominant in $G$** if
\[
\limsup_{t \to \infty} f_t(G, X, H, k) \neq 0.
\]

$k$-spectrum of $G$:

\[
Spec_k(G) = \{\text{dominant subgroups of } G\}
\]

**Main problem:** What is $Spec_k(G)$ for a given $G$?
**Generic subgroups**

For $k \in \mathbb{N}$ we say that a $k$-generated group $H$ is a **generic subgroup** of $G$ if a random $k$-generated subgroup of $G$ is isomorphic to $H$:

$$\limsup_{t \to \infty} f_t(G, X, H, k) = 1$$

In this case we say that $G$ has **unique random $k$-subgroups** ($URS_k$).

**Main Themes:**

1. For a given group $G$ and $k \in \mathbb{N}$ describe the spectrum $Spec_k(G)$;

2. Study groups with $URS$. 
Asymptotically Dominant Nielsen Property

A group $G$ generated by $X$ has asymptotically dominant Nielsen property if for every $k \in \mathbb{N}$ a random tuple $W = (w_1, \ldots, w_k) \in F(X)$ generates a free group and $W$ is a Nielsen of the group.

In groups with Dominant Nielsen property free groups are generic subgroups.
Examples of groups with DNP:

- Free groups [Jitsukawa]
- Pure Braid groups [Myasnikov, Ushakov]
- Hyperbolic groups [Gilman, Myasnikov, Osin]
- Groups admitting a non-trivial splitting as an amalgamated free product or HNN extension
Length Based Attacks in groups with DNP

In AAG scheme one chooses random subgroups:

\[ A = \langle a_1, \ldots, a_n \rangle, \quad B = \langle b_1, \ldots, b_m \rangle \]

Then solve the conjugacy equations of the type \( w^x = w^* \) in the group generated by \( C = \{a_1, \ldots, a_n, b_1, \ldots, b_m\} \) which is free on \( C \).

Length base attack!

But we need to know the length...
Computing the length

$G$ generated by $X$.

**Geodesic normal forms** in $G$:

$$w \rightarrow \bar{w}$$

if $\bar{w}$ is a shortest representative of $w$ (geodesic in the Cayley graph of $G$ relative to $X$).

Computing of geodesic normal forms in $G$ gives the length function $d$ (distance) in $G$.

Sometimes normal forms are not geodesic but **quasi-geodesic**.

This gives an approximation $d^*$ of the length function on $G$. 
Approximating the length in Braid Groups

[Dynnikov]

Asymptotically Dehornoy forms give some approximation $d^*$ of the length in braid groups $B_n$.

[Myasnikov, Shpilrain, Ushakov]

"Practical" approximation of the length in $B_n$ based on Dehornoy forms and heuristic algorithms.
Length functions in subgroups

$H$ is a subgroup of $G$ generated by $W$

The length $d_W$ in $H$ is different from the length $d_X$ induced from $G$.

How to realize the length attack on $H$ even if $H$ is free?

Possible if $H$ is quasi-isometrically embedded in $G$: $d_X$ is an approximation of $d_W$. 
Quasi-isometrically embedded subgroups

Conjecture:

Property of being quasi-isometrically embedded is asymptotically dominant in groups.

In hyperbolic groups generic subgroups are free and quasi-isometrically embedded.
Large subgroups

**Idea:** instead of long generators use "short" generators of sub-groups in $G$.

For a fixed $t \in \mathbb{N}$ we say that $t$-short subgroups converge to $G$ if "most" of the $t$-short subgroups are equal to $G$.

There are very effective attacks if the subgroup are equal to $G$. 
Subgroup Black Holes

Idea: Chose subgroups in the subgroup black hole
Good subgroups in Braid groups