Provable Security from Group Theory & Applications

CNS-1117679

Antonio R. Nicolosi

Stevens Institute of Technology

CNS-1117675

N. Fazio, W.E. Skeith, G. Baumslag, V. Shpilrain

City College of CUNY


A. Nicolosi N. Fazio

Diversifying Intractability Assumptions for Efficient Crypto

This project builds a foundation for provable crypto based on combinatorial group theory. Its core objectives are to identify distributional problems for non-commutative (possibly infinite) groups, establish evidence to their average-case hardness, and explore group-theoretic cryptographic constructions with enhanced functionalities.

Two-Pronged Approach

Group-theoretic learning problems

- Build on success of computational learning problems as source of intractability, e.g.,
  - *Learning Parity with Noise* (LPN)
  - *Learning With Errors* (LWE)
- Generalize to non-commutative setting:
  - ✓ ***Learning homomorphisms w/ noise in Burnside groups of exponent 3***

Distributional problems for infinite groups

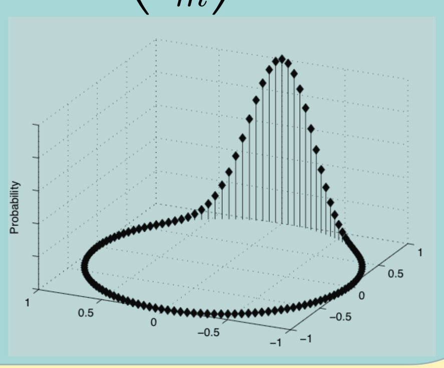
- Carve out hard-on-average problems from unsolvable algorithmic questions in combinatorial groups (e.g. *subgroup* problem)
- Identify suitable probability distributions that:
  - are efficiently sampleable over infinite groups
  - yield hard instances of underlying fundamental group-theoretic problems

Background: Learning With Errors (LWE)

- Idea: Small random perturbations ("errors") make easy learning problems into hard ones
- E.g., solving linear systems is $\Theta(n^3)$, but add noise, and best solution [BKW11] is $2^{\Theta(n/\log n)}$:

$$\text{Given } \mathbf{A} = \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix} \in \mathbb{Z}_q^{m\times n} \quad \mathbf{b} = \mathbf{A}\cdot\mathbf{x} + \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix}, e_i \sim \Psi_{c\sqrt{n}}$$

$$\text{Find } \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Z}_q^n \qquad \Psi_{c\sqrt{n}}:$$



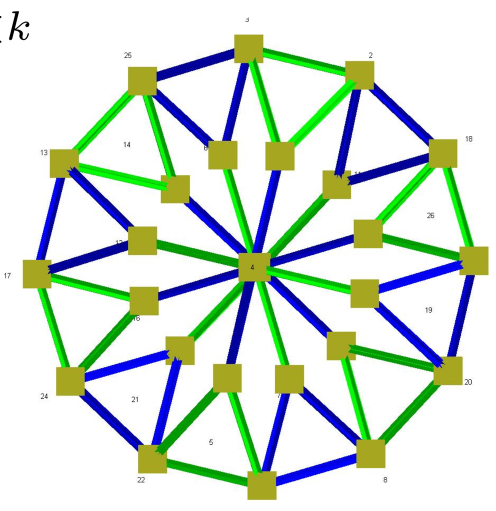
B_n: Burnside Groups of Exponent Three

- A finite non-commutative "generalization" of $\mathbb{Z}_3^n$
- "Most generic" group with n generators s.t.
  - $w^3 = 1, \forall w \in B_n$ (exponent condition)
- Normal form of B_n (with generators $x_1, \dots, x_n$):

$$\prod_{i=1}^{n} x_i^{\alpha_i} \prod_{i<j} [x_i, x_j]^{\beta_{i,j}} \prod_{i<j<k} [x_i, x_j, x_k]^{\gamma_{i,j,k}}$$

where $\alpha_i, \beta_{i,j}, \gamma_{i,j,k} \in \mathbb{Z}_3$,
$[x_i, x_j] \doteq x_i^{-1} x_j^{-1} x_i x_j$,
and $[x_i, x_j, x_k] \doteq [[x_i, x_j], x_k]$

- Order of B_n : $3^{n+\binom{n}{2}+\binom{n}{3}}$
- $|hom(B_n, B_r)| = 3^{n(r+\binom{r}{2}+\binom{r}{3})}$



B_2

LHN: Learning Homomorphisms w/ Noise

- Insight: At core, LWE is about hiding a linear function from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ by adding errors
- Idea: generalize linear functions to group homomorphisms, and hide them via noise
  - Learning Homomorphisms w/ Noise (LHN)
- Let G_n and P_n be groups, and $\varphi \xleftarrow{\$} hom(G_n, P_n)$
  - $hom(G_n, P_n)$: All homomorphisms from G_n to P_n
- Let Ψ_n be a "noise" distribution over P_n
- Let A_{φ,Ψ_n} be the distribution of "noisy samples"
  - $(a, b) \xleftarrow{\$} A_{\varphi,\Psi_n} \doteq a \xleftarrow{\$} G_n, e \xleftarrow{\$} \Psi_n, b \leftarrow \varphi(a)e$
- ✓ LHN assumption: $A_{\varphi,\Psi_n} \approx_{\text{PPT}} U(G_n \times P_n)$
  - LWE as special case: $G_n = \mathbb{Z}_q^n, P_n = \mathbb{Z}_q$
- ✓ B_n-LHN assumption: $G_n = B_n, P_n = B_r (r \lll n)$
  - $e \xleftarrow{\$} \Psi_n \doteq \sigma \xleftarrow{\$} \mathcal{S}_r, v_i \xleftarrow{\$} \mathbb{Z}_3\ (\forall i \in [r]), e \leftarrow \prod_{i=1}^{r} x_{\sigma(i)}^{v_i}$

Average-Case Hardness of B_n-LHN

- Main result: B_n-LHN is *random self-reducible*
  - Solving B_n-LHN when φ is *random* as hard as solving it when φ is arbitrary*
- Why does random self-reducibility matter?
  - Common trait of "standard" assumptions
  - Simplifies key generation and assessment of cryptanalytic resistance:
    - ➢ Either no* hidden homomorphism is secure, or all choices are good
- Other hardness results (in progress / planned):
  - Ruling out reductions to LWE with $q = 3$
  - Decision-to-search reduction (in progress)
  - Cryptanalytic assessment (future work)
  - Hardness under auxiliary info (future work)

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

Stevens Institute of Technology — The City College of New York