On the Notion of Pseudo-Free Groups

Ronald L. Rivest
MIT Computer Science and Artificial Intelligence Laboratory

TCC 2/21/2004

Outline

- Assumptions: complexity-theoretic, group-theoretic
- Groups: Math, Computational, BB, Free
- Weak pseudo-free groups
- Equations over groups and free groups
- Pseudo-free groups
- Implications of pseudo-freeness
- Open problems

Cryptographic assumptions

- Computational cryptography depends on complexity-theoretic *assumptions*.
- ∃ two types:
  - *Generic:* *OWF, TDP, P!=NP, ...*
  - *Algebraic:* *Factoring, RSA, DLP, DH, Strong RSA, ECDLP, GAP, WPFG, PFG, ...*
- We're interested in *algebraic* assumptions (about *groups*)

Groups

- Familiar algebraic structure in crypto.
- *Mathematical group* $G = (S,*)$: binary operation * defined on (finite) set S: associative, identity, inverses, perhaps abelian. Example: Z_n^* (running example).
- *Computational group* $[G]$ implements a mathematical group G. Each element x in G has one or more representations $[x]$ in $[G]$. E.g. $[Z_n^*]$ via least positive residues.
- *Black-box group:* pretend $[G] = G$.

Free Groups

- *Generators:* $a_1, a_2, \ldots, a_t$
- *Symbols:* generators and their inverses.
- *Elements* of free group $F(a_1, a_2, \ldots, a_t)$ are reduced finite sequences of symbols---no symbol is next to its inverse.

  $ab^{-1}a^{-1}bc$ is in $F(a,b,c)$; abb^{-1} is not.
- *Group operation:* concatenation & reduction.
- *Identity:* empty sequence ε (or 1).

Free Group Properties

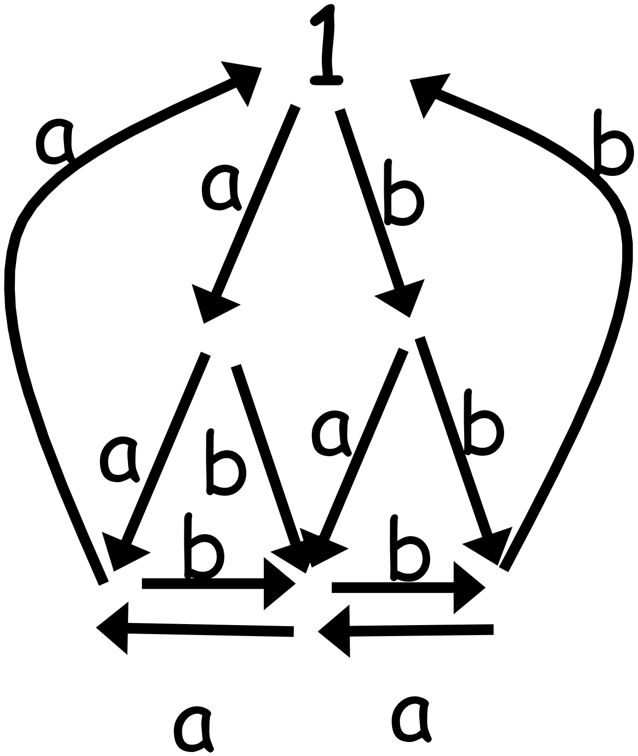
- Free group is infinite.
- In a free group, every element other than the identity has infinite order.
- Free group has no nontrivial relationships.
- Reasoning in a free group is relatively straightforward and simple; ≈ "Dolev-Yao" for groups…
- Every group is homomorphic image of a free group.

Abelian Free Groups

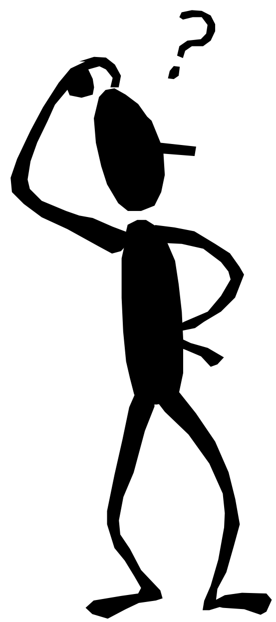
- There is also <u>abelian</u> free group
  $FA(a_1, a_2, \ldots, a_t)$,
  which is isomorphic to
  $Z \times Z \times \ldots \times Z$ (t times).
- Elements of $FA(a_1, a_2, \ldots, a_t)$ have simple canonical form:
  $a_1^{e1}a_2^{e2}\ldots a_t^{et}$
- We will often omit specifying abelian; most of our definitions have abelian and non-abelian versions.

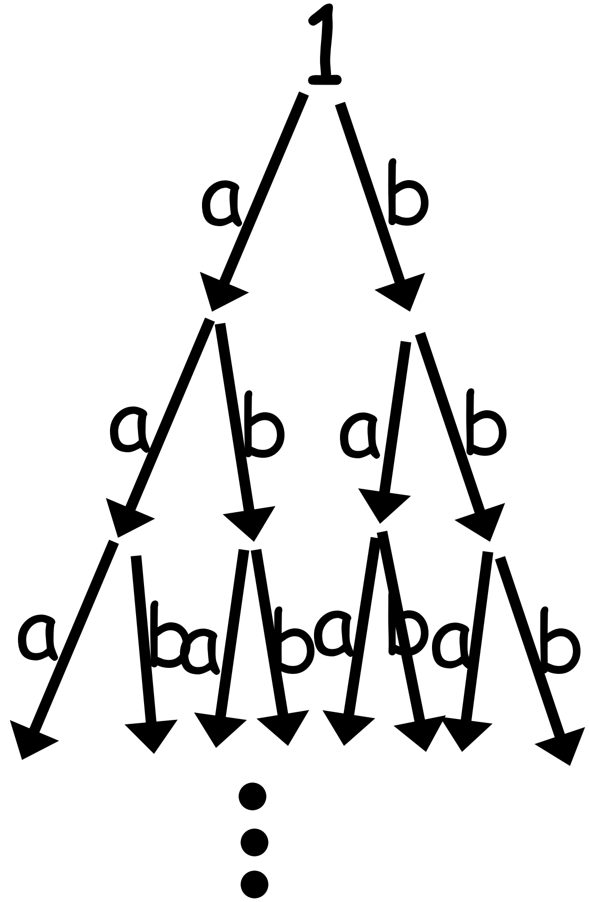
Pseudo-Free Groups (Informal)

- "A finite group is *pseudo-free* if it can not be efficiently distinguished from a free group."
- Notion first expressed, in simple form, in Susan Hohenberger's M.S. thesis.
- We give two formalizations, and show that assumption of pseudo-freeness implies many other well-known assumptions.



Cayley graph
of finite group





Cayley graph
of free group

Two ways of distinguishing

- In a *weak pseudo-free group* (WPFG), *adversary can't find any nontrivial identity involving supplied random elements:*

$$a^2 b^5 c^{-1} = 1 \qquad (!)$$

- *In a (strong) pseudo-free group (PFG), adversary can't solve nontrivial equations:*

$$x^2 = a^3 b$$

Weak Pseudo-freeness

- A family of computational groups $\{ G_k \}$ is weakly pseudo-free if for any polynomial t(k) a PPT adversary has negl(k) chance of:
  - Accepting $t(k)$ random elements of G_k,

    $$a_1, \ldots, a_{t(k)}$$

  - Producing any word w over the symbols

    $$a_1, \ldots, a_{t(k)}\, a_1^{-1}, \ldots, a_{t(k)}^{-1}$$

    when interpreted as a product in G_k using the obtained random values, yields the identity 1, while w does not yield 1 in the free group.
  - Adversary may use compact notion (exponents, straight-line programs) when describing w.

Order problem

- Theorem: *In a WPFG, finding the order of a randomly chosen element is hard.*
- Proof: The equation

$$a^e = 1$$

does not hold for any e in $FA(a)$. No element other than 1 in a free group has finite order.

Discrete logarithm problem

- <u>Theorem:</u> *In a WPFG, DLP is hard.*
- <u>Proof</u>: The equation

$$a^e = b$$

does not hold for any e in $FA(a,b)$; a and b are distinct independent generators, one can not be power of other.

Subgroups of PFG's

- Subgroup Theorem for WPFG's:
  If G is a WPFG, and g is chosen at random from G, then $\langle g\rangle$ is a WPFG. [not in paper]
- Proof sketch: Ability to find nontrivial identities in $\langle g\rangle$ can be shown to imply that g has finite order.
- ==> DLP is hard in WPFG even if we enforce "promise" that b is a (random) power of a .
- Similar proof implies that
  QR_n is WPFG when $n = (2p'+1)(2q'+1)$.

Equations in Groups

- Let x, y, … denote variables in group.
- Consider the equation

$$x^2 = a \qquad (*)$$

  This equation may be satisfiable in Z_n^* (when a is in QR_n), but this equation is *never* satisfiable in a free group, since reduced form of x^2 always has *even* length.
- Exhibiting a solution to (*) in a group G is another way to demonstrate that G is not a free group.

Equations in Free Groups

- Can always be put into form:

  $$w = 1$$

  where w is sequence over symbols of group and variables.
- It is decidable (Makanin '82) in PSPACE (Gutierrez '00) whether an equation is satisfiable in free group.
- Multiple equations equivalent to single one.
- For abelian free group it is in P. Also: if equation is unsatisfiable in FA() it is unsatisfiable in F().

Pseudo-freeness

- A family of computational groups $\{ G_k \}$ is **pseudo-free** if for any poly's t(k), m(k) a PPT adversary has negl(k) chance of:
  - Accepting $t(k)$ random elements of G_k,
  - Producing any equation
    $$E(a_1,\ldots,a_{t(k)},x_1,\ldots,x_{m(k)}):\ \ w = 1$$
    with $t(k)$ generator symbols and $m(k)$ variables that is *unsatisfiable* over $F(a_1,\ldots,a_{t(k)})$
  - Producing a solution to E over G_k, with given random elements substituted for generators.

Main conjecture

- Conjecture:
  { Z_n* } is a (strong) (abelian) pseudo-free group
- aka "Super-strong RSA conjecture"
- What are implications of PFG assumption?

RSA and Strong RSA

- <u>Theorem:</u> *In a PFG, RSA assumption and Strong RSA assumptions hold.*
- <u>Proof</u>: For $e>1$ the equation

$$x^e = a$$

is not satisfiable in FA(a)
(and also thus not in F(a)).

Taking square roots

- Theorem: *In a PFG, taking square roots of randomly chosen elements is hard.*
- Proof: As noted earlier, the equation

$$x^2 = a \qquad (*)$$

has no solution in FA(a) or F(a).
- Note the importance of forcing adversary to solve (*) for a *random a;* it wouldn't do to allow him to take square root of, say, 4 .

Computational Diffie-Hellman ☹

- CDH: Given g, $a = g^e$, and $b = g^f$, computing $x = g^{ef}$ is hard.
- <u>Conjecture:</u> CDH holds in a PFG.
- <u>Remark:</u> This seems natural, since in a free group there is no element (other than 1) that is simultaneously a power of more than one generator. Yet the adversary merely needs to output x; there is no equation involving x that he must output.

Open problems

- Show factoring implies $Z_n{}^*$ is PFG.
- Show CDH holds in PFG's.
- Show utility of PFG theory by simplifying known security proofs.
- Determine is satisfiability of equation over free group is decidable when variables include exponents.
- Extend theory to groups of known size (e.g. mod *p*), and adaptive attacks (adversary can get solution to some equations of his choice for free).

(THE END)

Safe travels!