Charles E. Schmidt College of Science

Defeating p-attack in non-abelian DLP

Krishna Thapa Magar, Ivana Ilic, Spyros Magliveras

Mathematical Sciences; Florida Atlantic University

Non-abelian Discrete Logarithm Problem (DLP) can be solved efficiently in the group PSL(2,p) [Projective Special Linear group] by a method called p-attack, if the p-depth of generators is minimum. But as we increase p, we can find generators whose p-depth is higher. As a result, p-attack can be defeated.
Keywords: Discrete log, Non-abelian group, p-attack, p-depth.

Defeating p −attack in non-abelian discrete logarithm problem

Krishna Thapa Magar *[1], Ivana Ilić[2] and Spyros Magliveras[1]

[1]Department of Mathematical Sciences, FAU ; [2]Department of Mathematics, Edison State College

Introduction and definitions

Discrete logarithm problem

G - finite cyclic group generated by an element α

β - an element from group G

The discrete logarithm problem is to find the non-negative integer x such that $\alpha^x = \beta$.

- Cryptographic primitives are designed based on intractability of the discrete logarithm problem (DLP)

Motivation for exploring non-abelian groups and generalized DLP

- Algorithms for solving DLP in cyclic groups:

-Baby Step-Giant Step, Pollard Rho, Pohlig-Hellman, Index calculus

-Shor's polynomial time algorithm for prime factorization and discrete logarithm

Generalized discrete logarithm problem

- Lee C. Klingler, Spyros S. Magliveras, Fred Richman, Michal Sramka, *Discrete logarithms for finite groups*, 2009.

Definition1: *Let G be a finite group generated by $\alpha_1, \ldots, \alpha_t$ i.e. $G = \langle \alpha_1, \ldots, \alpha_t \rangle$. Given $\beta \in G$, the* ***generalized discrete logarithm problem*** *for β with respect to $\alpha = \langle \alpha_1, \ldots, \alpha_t \rangle$ is : Find a positive integer k and kt-tuple of non-negative integers $x = (x_{11}, \ldots, x_{1t}, \ldots, x_{k1}, \ldots, x_{kt})$ such that $\beta = \prod_{i=1}^{k} (\alpha_1^{x_{i1}} \cdots \alpha_t^{x_{it}})$.*

Algebra of exponent

Let $x \in \mathbb{Z}^+$ and $\alpha = (\alpha_1, \ldots, \alpha_t)$ be ordered set of generators of group G $|\alpha_i| = n_i$, $n = n_1 \cdots n_t$. Write $x = x_1 n^{k-1} + x_2 n^{k-2} + \cdots + x_{k-1} n + x_k$. $(x_1, \ldots, x_k)$ are digits of x with respect to radix n.

For each x_i, let $(x_{i1}, \ldots, x_{it})$ be the digits of x_i with respect to mixed radix $(n_1, \ldots, n_t)$ so that $0 \le x_{ij} < n_j$. Then

$$[\alpha_1, \ldots, \alpha_t]^x \stackrel{\text{def}}{=} \prod_{i=1}^{k} [\alpha_1, \ldots, \alpha_t]^{x_i} \stackrel{\text{def}}{=} \prod_{i=1}^{k} (\alpha_1^{x_{i1}} \cdots \alpha_t^{x_{it}}).$$

Example: Consider a group $G = \langle \alpha, \beta \rangle$ generated by two elements α and β where $n_1 = o(\alpha) = 8$ and $n_2 = o(\beta) = 5$ so that $n = n_1 n_2 = 40$. We want to compute $[\alpha, \beta]^{1011}$.

First we write 1011 with respect to radix $n = 40$ representation:
$1011 = 25 \times 40^1 + 11 \times 40^0$. Say $(x_1, x_2) = (25,11)$.

Now we write each of x_1 and x_2 with respect to mixed radix $(n_1, n_2) = (8,5)$ as follows:

$$25 = 5 \times 5 + 0 \times 5^0$$
$$11 = 2 \times 5 + 1 \times 5^0$$

So $(x_{11}, x_{12}) = (5,0)$ and $(x_{21}, x_{22}) = (2,1)$.

So that 1011 corresponds to the vector (5,0,2,1) and hence $[\alpha, \beta]^{1011} = \alpha^5 \beta^0 \alpha^2 \beta^1$.

Addition:

Let G $= \langle \alpha_1, \ldots, \alpha_t \rangle$ be a finite non-abelian group. Then for $x, y \in \mathbb{Z}$, $[\alpha_1, \ldots, \alpha_t]^{x \oplus y} = [\alpha_1, \ldots, \alpha_t]^x \, [\alpha_1, \ldots, \alpha_t]^y$.

p −attack in non-abelian discrete logarithm

- The non-abelian group suggested by Spyros S. Magliveras was $G = PSL(2,p)$, $p \neq 2$.
- In her 2010 Ph.D. dissertation Ivana Ilić proved that generalized DLP in the group $PSL(2,p)$ with respect to specific generating pairs (α, β) : $\alpha = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ of order p can be solved efficiently.
- Following proposition provides a solution:

Proposition1: *For given group $G = PSL(2,p) = \langle \alpha, \beta \rangle$; $\alpha = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an element of G. Then there exists a non-negative integer $n < p$ such that $nd - b \neq 0$ over $\mathbb{Z}_p$, such that the 4-tuple (i, j, k, l) with*

$$i = n,$$
$$j = (1-d)(nd-b)^{-1},$$
$$k = b - nd,$$
$$l = (1-d)(nc-a)(nd-b)^{-1} + c$$

provides a solution to $M = \alpha^i \beta^j \alpha^k \beta^l$.

- Successful cryptanalysis of the GDLP in $G = PSL(2,p) = \langle \alpha, \beta \rangle$, when at least one of the two generators is of order p, rests on reduction to the basic case where the generators are the canonical elements $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. We call a cryptanalytic attack of this type a basic p −attack.

p −attack

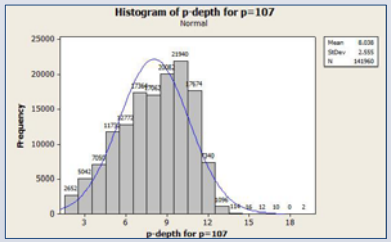
- **What if none of the generators are of order p ?**
- **Definition2:** *Suppose that $G = PSL(2,p) = \langle \alpha, \beta \rangle$. The* ***p-depth*** *of (α, β), denoted by $pd(\alpha, \beta)$, is the length of the shortest possible word in α and β which is of order p as an element of G.*
- **Proposition2:** *Suppose that $G = PSL(2,p) = \langle \alpha, \beta \rangle$ where orders of α and β are relatively prime to p and suppose that $P = w_p(\alpha, \beta)$, is a word in α and β which has order p as an element of G. Then $G = \langle \alpha, P \rangle$ or $G = \langle \beta, P \rangle$.*
- **Definition3:** *Proposition 2 guarantees us that the generalized DLP can be solved in $G = PSL(2,p) = \langle \alpha, \beta \rangle$ where none of the generators α and β are of order p,* ***not necessarily efficiently.*** *This Ilić's method of solving GDLP is called a* ***p −attack.***
- However the success of p −attack depends on a low value for $pd(\alpha, \beta)$.

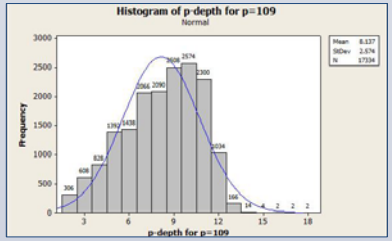
Defeating p −attack

- If we assume $G = PSL(2,p) = \langle \alpha, \beta \rangle$ where α and β both are of order $\frac{p-1}{2}$, we collect experimental evidence that the average p-depth is at least $\log_2 p$ with some generating pairs having extremely high p-depth.
- Since p–depth is invariant under conjugation, we achieve considerable computational gain by selecting representatives of the orbits under conjugation of generating pairs in $X \times X$, where X is the set of all elements of order $\frac{p-1}{2}$ in G.
- Our conjecture is that we can always defeat a p–attack by taking p sufficiently large and α and β appropriate generators of high p –depth.

Experimental results

p	η (# of gen pairs)	Max p-depth	Mean p −depth	p	η (# of gen pairs)	Max p-depth	Mean p-depth
11	56	8	4.607	61	1888	14	7.431
13	22	9	5.636	67	13000	17	7.447
17	120	12	5.917	71	19872	19	7.461
19	306	13	5.922	73	5112	17	7.624
23	1050	13	6.059	79	22176	17	7.651
29	486	13	6.370	83	64800	19	7.682
31	928	14	6.569	89	17400	17	7.843
37	630	12	6.765	97	12160	18	7.951
41	1248	15	6.804	101	19800	16	8.015
43	2952	16	6.814	103	51712	18	8.009
47	10890	16	6.916	107	141960	19	8.038
53	3672	15	7.095	109	17334	18	8.137
59	22344	18	7.223				





Conclusion

- For a generating pair (α, β), even if an oracle is available to provide $k = pd(\alpha, \beta)$, the time complexity for finding the shortest word $w_p(\alpha, \beta)$ of order p is 2^k.
- Since *average p–depth* $> \log_2 p$, the worst case complexity of finding $w_p(\alpha, \beta)$ for a generating pair (α, β) of average p–depth is at least $2^{\log_2 p} = p$.
- Since the cryptographers would choose a large p, say of size 2^{100}, finding $w_p(\alpha, \beta)$ by brute force would be infeasible.
- Thus we can defeat p–attack by selecting generating pairs with p–depth $>$ average p–depth.
- We may call generating pairs with this property, ***secure generating pairs***.

Open questions

- Exploring hardness of the generalized DLP with respect to different generating tuples in different non-abelian finite groups.
- Building cryptographic primitives based on the hardness of the computation of the generalized DLP.
- Developing algorithms for attacking the generalized DLP in finite non-abelian groups.

References

1. Lee C. Klingler, Spyros S. Magliveras, Fred Richman, Michal Sramka, *Discrete logarithm for finite groups,* Computing **85** (2009), pp. 3-19.
2. Ivana Ilić, Spyros S. Magliveras, *Weak discrete logarithm in non-abelian groups.* J. Comb. Math and Comb. Comput., (JCMCC) **74** (2010).
3. Douglas R. Stinson, *Cryptography: Theory and Practice. Third Edition.* Chapman & Hall/CRC (2006).
4. Alfred Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography,* CRC Press (1996).

Contact

- *Krishna Thapa Magar*, Department of Mathematical Sciences, Florida Atlantic University. Email: kthapama@fau.edu
- *Ivana Ilić*, Department of Mathematics, Edison State College. Email: iilic@edison.edu
- *Spyros Magliveras*, Department of Mathematical Sciences, Florida Atlantic University. Email: spyros@fau.edu