Outline

Collisions algorithms for DLP

Pollard - rho

Recall Discrete Logarithm Problem (DLP)

---

p is odd prime. $G = \langle g \rangle$ of order p.

Given p, g and $h \in G$.

Find e such that $g^e = h$

Recall Baby-Step / Giant-Step

- Create two lists L_1, L_2 each of size $\sqrt{p}$
- Running time is $O(\sqrt{p})$

Motivation for collision algorithm to solve DLP is to remove the $\sqrt{p}$ space requirement

Proposition 2.21 (Shanks's Babystep–Giantstep Algorithm). *Let G be a group and let $g \in G$ be an element of order $N \geq 2$. The following algorithm solves the discrete logarithm problem $g^x = h$ in $\mathcal{O}(\sqrt{N} \cdot \log N)$ steps using $\mathcal{O}(\sqrt{N})$ storage.*

(1) *Let $n = 1 + \lfloor \sqrt{N} \rfloor$, so in particular, $n > \sqrt{N}$.*

(2) *Create two lists,*

$$\text{List 1:} \quad e,\ g,\ g^2,\ g^3,\ \ldots,\ g^n,$$
$$\text{List 2:} \quad h,\ h \cdot g^{-n},\ h \cdot g^{-2n},\ h \cdot g^{-3n},\ \ldots,\ h \cdot g^{-n^2}.$$

collision

(3) *Find a match between the two lists, say $g^i = hg^{-jn}$.*

(4) *Then $x = i + jn$ is a solution to $g^x = h$.*

Pollard's Rho algorithm (a collision algorithm)

Suppose $f : S \to S$ a random mapping of a finite set S and itself. $|S| = n$

Take any $x_0 \in S$. Compute $x_{i+1} = f(x_i)$

We have $x_0, x_1, x_2, \ldots\ldots,$ called pseudo-random walk.

Since S is finite, we have

$$x_i = x_j \quad \text{for some } i, j.$$

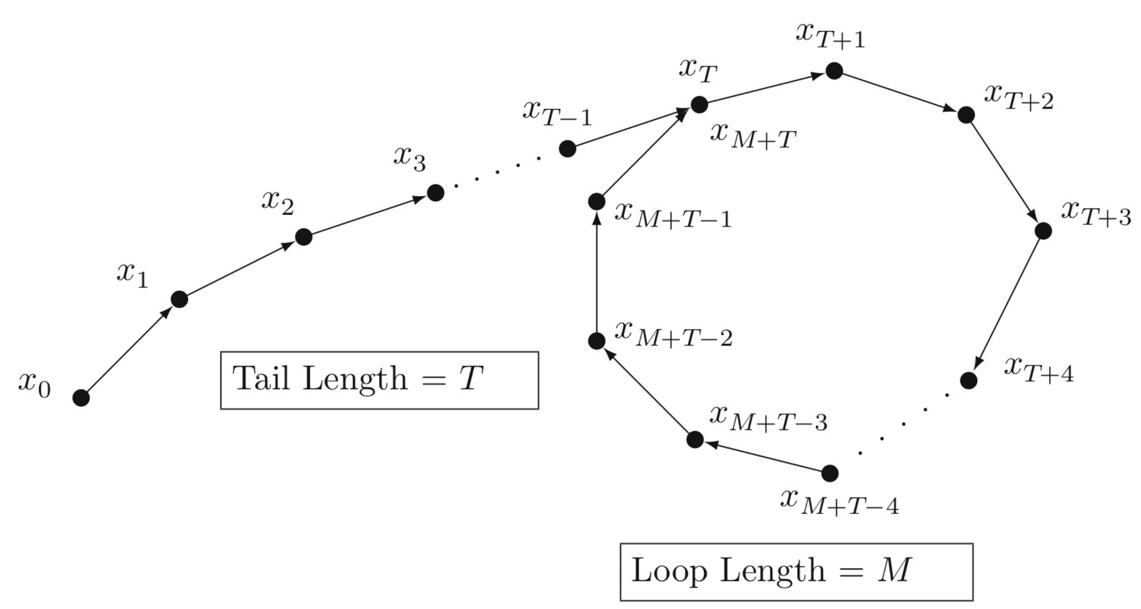

Figure 5.1: Pollard's ρ method

By Birthday Paradox, we obtain a collision after an expected number of $\sqrt{\frac{\pi n}{2}}$. $E[T+M] = \sqrt{\frac{\pi n}{2}}$

Floyd's cycle algorithm (Idea)

$x_0 = y_0$

$x_{i+1} = f(x_i)$

$y_{i+1} = f(f(y_i))$

When x_i is equal to y_i, we found the collision.
without having to store any values.

Note that $y_i = x_{2i}$

Is there i such that $x_i = x_{2i}$ if there exists collision?

We know from the cycle that

$x_i = x_j$ iff i and $j \geq T$ and M divides $j-i$

If $x_i = x_{2i}$ then i and $2i \geq T$ and $M \mid i$

i will be the first value $\geq T$ such that it is divisible by M. Consider the sequence

$T, \quad T+1, \quad T+2, \quad \cdots, \quad T+M-1$

Take modulo M.

$a, \quad a+1, \quad a+2, \quad \cdots, \quad a+M-1$

There are M values. One of them must be 0.

So, $\exists\, i$ such that $x_i = y_i = x_{2i}$ when collision exists.

Pollard-rho's algorithm

If $f: S \to S$ is random mapping of a finite set.

(1) Suppose $x_0, x_1, \ldots,$ is the pseudo-random walk where $x_{i+1} = f(x_i)$. Then $\exists\ 1 \le i \le T+M$ such that

$$x_{2i} = x_i$$

where T is length of the tail and M is length of cycle.

(2) $E(T+M) = \sqrt{\frac{\pi}{2}|S|}$ (By Birthday Paradox)

Application on solving DLP

Solve $g^e = h \mod p$

Idea: If $g^i h^j = g^k h^l \mod p$ (given i, j, k, l)

then $g^{i-k} = h^{l-j} \mod p$

$$g^{i-k} = g^{e(l-j)} \mod p$$

$$i-k \equiv e(l-j) \mod p-1 \quad (*)$$

Solve e from $(*)$ given i, j, k, l

Probabilistic method to solve DLP (version 1)

$L1: g^i$ for some random i $\quad 0 \le i \le p-1$

$L2: hg^j$ for some random j $\quad 0 \le j \le p-1$

If $|L_1|$ and $|L_2| = O(\sqrt{p})$ then there is a high probability that they will have collisions.

Comparison between this and Shanks BSGS

1. BSGS : Deterministic
   This : Probabilistic
2. Same space complexity
3. BSGS : computation of g^i or hg^i is g times previous value

   This : each computation of g^i can't use the previous value.

Probabilistic Method to solve DLP (version 2)

Use Pollard-rho algorithm: $g^e = h \mod p$

$$f(x) = \begin{cases} gx & \text{if } 0 \le x < p/3, \\ x^2 & \text{if } p/3 \le x < 2p/3, \\ hx & \text{if } 2p/3 \le x < p. \end{cases}$$

* It is unknown that whether this function is random enough to guarantee a collision after $\sqrt{\frac{\pi}{2}p}$ steps.

$x_0 = y_0$

$x_{i+1} = f(x_i)$

$y_{i+1} = f(y_i)$

Suppose $x_s = y_s$

Write $x_s = g^\alpha h^\beta$

$y_s = g^\gamma h^\delta$

Then solve $\alpha - \gamma \equiv e(\beta - \delta) \mod p-1$

When compute x_i, y_i, keep track of $\alpha_i, \beta_i, \gamma_i, \delta_i$ where

$$x_i = g^{\alpha_i} h^{\beta_i}$$

$$y_i = g^{\gamma_i} h^{\delta_i}$$

$$\alpha_{i+1} = \begin{cases} \alpha_i + 1 & \text{when } 0 \le x < p/3 \\ 2\alpha_i & \text{when } p/3 \le x < 2p/3 \\ \alpha_i & \text{when } 2p/3 \le x < p \end{cases}$$

$$\beta_{i+1} = \begin{cases} \beta_i & \text{when } 0 \le x < p/3 \\ 2\beta_i & \text{when } p/3 \le x < 2p/3 \\ \beta_i + 1 & \text{when } 2p/3 \le x < p \end{cases}$$

$$\gamma_{i+1} = \left\{ \vphantom{\begin{matrix} a \\ b \\ c \end{matrix}} \right.$$

$$\delta_{i+1} = \left\{ \vphantom{\begin{matrix} a \\ b \\ c \end{matrix}} \right.$$

Challenge:

Pollard rho algorithm is used to solve DLP.

Can we use same collision algorithm strategy to factor $N = pq$, where p, q are odd primes

See Homework 11, Question 3