Reminder: we want $f: \langle P \rangle \to \langle P \rangle$ (cycle group generated by P)

the Lattice random

In the forward, we used the following: take $x(W_i)$ (call this $s(W_i)$) integer mod 3,

the $W_{i+1} = \begin{cases} W_i + P & \text{if } s(W_i) = 0 \\ W_i + P_i & \text{if } s(W_i) = 1 \\ -W_i & \text{if } s(W_i) = 2 \end{cases}$

Last lecture: $W_{i+1} = b_{i+1} P + c_{i+1} P_i$

for b_{i+1}, c_{i+1} depending on $x(W_i)$

We want to do this cheaper, the a double-scalar multiplication is more costly than this scheduled method (i.e. the one from the forward)

Solution: addition walks

Look to (mod 2^n) different addition steps S_i, $0 \le i < n$ with $S_i = 2^i P$ for some i.

and define

$W_{i+1} = W_i + S_{x(W_i) \bmod n}$ (mod 2^n)

$x(W_i)$ selects the next step;

each step only costs an addition.

More structured (100 instead of 10, longer in the 2^n case) makes the walk more random

How is this hardness work? How much worse is it vs 100?

$f(W_0) = f(W_T) = T$

I simply break T from W_0 if $T = W_0 + S_{x(W_0)}$

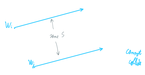
Then on $N = \mathrm{ord}(P)$ walks for T

Go to chance of getting to T,

$\frac{1}{N}$ chance of starting at right step.

have for $f(W_T) = T$

Note: the also requires the step to be different (meaning $W_i \neq W_j$, $i \neq j$ so we don't collision on a step that we just taken)



What is the effect of these add-collisions? (probably the same S_i, leading into another $\Rightarrow$ or collision)

$\mathbb{E}_{W_0} \quad \frac{1}{N} \cdot \frac{1}{N} \cdot \frac{1}{N} \cdot \frac{1}{N} = \sum_{W_0 \in G} \frac{1}{N^4} = \frac{1}{N^3} = \frac{1}{N^3} - \frac{1}{N^4} = \left(1 - \frac{1}{N}\right)\frac{1}{N^3}$

$= (x, \ldots, y)$ (the results $\{x, \ldots, y\}$ $\to$ make $\Rightarrow$) — depends on number of unique steps S_i

$\left(1 - \frac{1}{N}\right)\frac{1}{N^3}$ — depends on number of unique steps S_i

This is low by $\left(1 - \frac{1}{N}\right)$ factor. The the chance of collision at T of a truly random walk, which is $\frac{1}{N^3}$.

So, we lose some randomness.

Note: T is arbitrary, we're trying to collide anywhere! So the probabilities get multiplied by N for finding a collision somewhere, so $\left(1 - \frac{1}{N}\right)\frac{1}{N}$ vs $\frac{1}{N}$

$\left(\text{vs } \left(1 - \frac{1}{N^2}\right)\frac{1}{N^2}\right)$

This gets into $\sqrt{\pi N}$ at $\sqrt{\frac{\pi N}{2(1-\frac{1}{N})}}$ $\left(\text{vs } \sqrt{\frac{\pi N}{2(1-\frac{1}{N^2})}}\right)$

So the attack takes $\frac{1}{\sqrt{1-\frac{1}{N}}}$ more steps.

Good tradeoff if weight steps (or small in order the is, but never very bounded by pre-computing & storing S_i (more a fixed size overhead))

Edwards curves vs Weierstrass curve for attacks: Easy to convert an regular curves: $(X:Y:Z) = (\lambda X : \lambda Y : \lambda Z)$ because we need unique representation of an point, so we're using affine coordinates

The, Weierstrass curves are cheaper to work on.

However, the attacks on we (traditional approaches) don't work with relation from work but for the

---

Defining DLP: in a group, $\mathbb{G}$ is written the $O(\sqrt{N})$

How about DDH? (Decisional Diffie-Hellman problem)

Given P, aP, bP, cP, decide $cP = (ab)P$

Take a look at N, e.g. $N = 6 = 2 \cdot 3$. (or $N = 2 \cdot q$, for q a prime)

In this case, Jacobian mod N preserves even and odd, e.g.

$\beta \equiv 2 \bmod 6$

If at least one of a & b is even, the a & b even $\to$ the case.

So, a lot of things we can solve the DDHP.

If c is random, the fails with 50% chance, else it always fails.

How to test this? If $a = 2a'$, the $\frac{N}{2}(aP) = \frac{N}{2}(2a'P) = a'(NP) = \mathcal{O}P$ (from N is the order of the mod N Jacobian)

Until if $a = 2a' + 1$, the

$\frac{N}{2}(aP) = \frac{N}{2}(2a'+1)P = a'NP + \frac{N}{2}P = \frac{N}{2}P \neq \mathcal{O}P$ (by the definition of order / because of primality)

Thus, we can test with expense of multiplying by $\frac{N}{2}$. The return N larger.

Thus, we do not want even.

How about $N = 3 \cdot q$?

Normal (a mod 3) (b mod 3) results (mod 3) for DDH triple to be valid. Test where $\frac{N}{3}(aP) = \frac{N}{3}(\underbrace{3a'+a_1}_{a_1 \in \{1,2\}})P = \left(\frac{N}{3}a_1\right)P$

Since one only a resolution, we can brute force

get a_1, b_1, c_1 that satisfy DDH mod 3.

Hence for $5, 7, 11, \ldots$

Non-Jacobi attack on DLP?

For $N = 2 \cdot 3$, I can now get $a \bmod 2$

$a \bmod 3$

Pohlig-Hellman algorithm

Tonelli-Cantelli theorem

Chinese remainder theorem $\longrightarrow$ Pick $N = \prod p_i^{e_i}$ with p_i prime, $p_i \neq p_j$, $e \geq 1$, the a is uniquely given mod N by

$a \equiv a_1 \bmod p_1^{e_1}$

$a \equiv a_2 \bmod p_2^{e_2}$

$a \equiv a_k \bmod p_k^{e_k}$

by the Chinese remainder theorem (CRT)

Now, $N = 2 \cdot 3$, then look in polynomial time CRT compute a mod N

The work for any composite N — provided that we can get a mod $p_i^{e_i}$

Note: we do not want to brute-force in a set of $p_i^{e_i}$ because is out of $p_i^{e_i}$ because is computations of size p_i

Also we do not we use the BSGS or Pollard-rho is usually those small DLPs.