$p = 2\tilde{p} + 1$

do {

generate random prime $\tilde{p}$

$n := 2\tilde{p} + 1$

} while (n is not a prime)

$p := n$,

DLP $\quad \mathbb{F}_p^* = \{1, 2, \ldots, p-1\}, \cdot)$

take g which is random in $\mathbb{F}_p^* \setminus \{1\}$

$\tilde{g} := g^2 \pmod p$

if $\tilde{g} \neq 1 \pmod p$ then $\operatorname{ord} \tilde{g} = \tilde{p}$

take random $x \in \{1, 2, \ldots, \tilde{p}-1\}$

$y = \tilde{g}^x \pmod p$

$y \in \langle \tilde{g} \rangle$

$|\mathbb{F}_p^*| = p - 1 = 2 \cdot \tilde{p}$

$\text{Pollard-}\rho(\tilde{g}, y, \tilde{p}, p) \to x'$

$x' = x \pmod{\tilde{p}}$