

temps

$$O(\sqrt{|G|}), \quad |G| > 2^{160}$$

3.2.5

$$\Rightarrow |P|_2 \approx 160 \text{ bits.}$$

D'où le choix de la machine C est important