③ c) Note: Most of this is taken from Luca De Feo's paper, I tried to understand it, ~~but~~ If you considere this plagiarism, I'm OK with it.

If ρ has a length m, $\rho = (\sigma_1, \dots, \sigma_m)$, we have

$$\rho(g) = \exp_g\left(\prod \sigma_i\right)$$

for any $g \in G$. Since the order of σ_i does not matter, ~~its~~ as we can see above, we only consider how many times each element of D is in ρ. The protocol therefore resembles our well-known Diffie-Hellman KE.

To achieve the same level of security, we need $\rho_A(g)$ and $\rho_B(g)$ to be uniformly distributed. Since from $\boxed{b)}$ the graph from the previous points is an expander, and, as defined in $\boxed{a)}$, D generates $(\mathbb{Z}/p\mathbb{Z})^*$, we have most of that condition satisfied. In order to achieve better uniformity, walks must have legth $\approx \log p$. ~~To the~~

To have a big enough key space, we must have

$$|D| \approx \frac{\log p}{\log\log p}$$

, since, as mentioned earlier, a secret route is defined by the number of times each element of D is in $\rho(g)$