1 Trying to define the attacker goal

We think of an attacker $\mathcal{A}$ trying to seal an amount T of "fake sealed space" (for short - fake space) (we think of the unit being the size of the larget allowable sector, so if that is n, we actually mean Tn bytes). meaning that these bytes are not correctly encoded, the most natural example - a sequence of zeroes that has been placed at the end of the replica instead of the real values.

We have the parameter λ, of the amount of checks done during porep. We think of $\mathcal{R}$ as the random oracle giving the challenges as function of the seed (in the non-interactive case, the seed will be combined root of the replica and data, in the interactive case the seed comes from a ticket on chain). We wish to lower bound the expected number of queries t to $\mathcal{R}$ to generate T fake space. This corresponds to the number of porep generating attempts.

We assume $\mathcal{A}$ always tried to seal sectors of maximum allowed size.

$\mathcal{A}$ can make a choice ϵ for how much fake space to include in a replica.

We analyze the optimal choice of ϵ given λ.

Denote $\gamma = 1 - \epsilon$. The expected amount of new fake space in an attempt is

$$\epsilon \cdot \gamma^{\lambda} = (1-\gamma) \cdot \gamma^{\lambda} = \gamma^{\lambda} - \gamma^{\lambda+1}$$

The derivative w.r.t. γ is

$$\lambda\gamma^{\lambda-1} - (\lambda+1)\gamma^{\lambda}$$

Solving for zero we have

$$\lambda\gamma^{\lambda-1} - (\lambda+1)\gamma^{\lambda} = 0$$

iff

$$\gamma = \frac{\lambda}{\lambda+1}$$

We get that the expected added fake space in each try is $\Omega(1/\lambda)$ which means that the number of tries t in this model is not exponential but $O(T/\lambda)$.

Obtaining a percentage instead of absolute amount We could perhaps say the goal of the attacker is to obtain fake space that is a certian percentage of the space on the power table rather than an absolute number. In which case they would have to use a larger ϵ and then we could say num of tries is exponential in λ (to fill in details here..)

2 Interactive vs noninteractive

tl;dr:The point we make here: For a given value of λ interactive mode is always at least as secure as noninteractive (and potentially more secure). *Security* here precisely means the cost of putting a certain amount of fake space on chain (i.e. in the power table).

In the interactive model we can assume $\mathcal{A}$ must put a deposit D after comitting to the replica and before seeing the seed, and loses the deposit if any of the λ queries land on the ϵ-fraction of fake space in their committed replica. In this setting, in addition to the expected cost of t queries to $\mathcal{R}$, $\mathcal{A}$ will pay the cost of $D \cdot (t - T/\epsilon)$ for the failed attempts.

Predictability of tickets An $\mathcal{A}$ we much power of the chain might have a certian ability to predict the seed value from the ticket in advance. Note that in the worst case that $\mathcal{A}$ has total predictability of the tickets; his cost is still at least as high as in the non-interactive case, where he only pays for the queries to $\mathcal{R}$.