Lemma. *In SRLC1 (Section 5.3 and Algorithm 7), the chosen* m *fulfills* $m = O\left(\kappa \log^2(\kappa) \log\left(\epsilon_F^{-1}\right)\right)$.

The expression used to choose m (Algorithm 7, GenParams, line 2) can be bounded as follows:

Since $0 < \epsilon_F < 1$ and $1 < \kappa$, we have:

$$\begin{aligned}
& 1 - \prod_{i=1}^{\kappa} \left(1 - \left(1 - \frac{3}{\kappa}\right)^{m-i+1}\right) \\
\leq\ & 1 - \prod_{i=1}^{\kappa} \left(1 - \left(1 - \frac{3}{\kappa}\right)^{m-\kappa+1}\right) \\
\leq\ & 1 - \left(1 - \kappa \left(1 - \frac{3}{\kappa}\right)^{m-\kappa+1}\right) \\
=\ & 1 - \left(1 - \left(1 - \frac{3}{\kappa}\right)^{m-\kappa+1}\right)^{\kappa} \\
\leq\ & \kappa \left(1 - \frac{3}{\kappa}\right)^{m-\kappa}
\end{aligned}$$

Therefore, $\kappa(1 - \frac{3}{\kappa})^{m-\kappa} \leq \epsilon$ suffices for the expression in GenParams to be fulfilled.

We also have:

$$\begin{aligned}
& \kappa \left(1 - \frac{3}{\kappa}\right)^{m-\kappa} \leq \epsilon_F \\
\Leftrightarrow\ & \log\left(\kappa \left(1 - \frac{3}{\kappa}\right)^{m-\kappa}\right) \leq \log(\epsilon_F) \\
\Leftrightarrow\ & \log(\kappa) + (m-\kappa) \log\left(1 - \frac{3}{\kappa}\right) \leq \log(\epsilon_F) \\
\Leftrightarrow\ & (m-\kappa) \log\left(1 - \frac{3}{\kappa}\right) \leq \log(\epsilon_F/\kappa) \\
\Leftrightarrow\ & m - \kappa \geq \frac{\log(\epsilon_F/\kappa)}{\log\left(1 - \frac{3}{\kappa}\right)} \\
\Leftrightarrow\ & m \geq \frac{\log(\epsilon_F/\kappa)}{\log\left(1 - \frac{3}{\kappa}\right)} + \kappa = \frac{\log(\epsilon^{-1}\kappa)}{-\log(1 - \frac{3}{\kappa})} + \kappa
\end{aligned}$$

Since $\frac{\log\left(\epsilon_F^{-1}\kappa\right)}{-\log\left(1-\frac{3}{\kappa}\right)} = O\left(\kappa \log^2(\kappa) \log\left(\epsilon_F^{-1}\right)\right)$ and we choose the smallest m possible for algorithm 7, we get $m = O\left(\kappa \log^2(\kappa) \log\left(\epsilon_F^{-1}\right)\right)$.