1. Implement linear encryption (BBS cryptosystem) using the following template \[ \text{https://courses.cs.ut.ee/MTAT.07.014/2018_fall/uploads/Main/linear_enc_template.txt} \]. For simplicity we will use Schnorr’s group instead of a pairing group. (4pt)

2. Prove IND-CPA security of linear encryption. More precisely, assume that \((p, G, G_{\cdot \cdot}, g) \leftarrow \text{Setup}(1^\kappa)\) is \((\tau', \varepsilon')\)-DLIN secure and show that then the linear encryption is \((\tau, \varepsilon)\)-IND-CPA secure. Relation between \((\tau', \varepsilon')\) and \((\tau, \varepsilon)\) should be efficient.

**Hint:** Look up the IND-CPA proof of Elgamal - idea is the same. (5pt)