# Mögliche darstellbare Fehler-Szenarien:

Alice

* Alice wählt immer nur dieselbe Polarisation/ dieselben Datenbits
  + Wenn von Eve erkannt, kann Eve mithören, ohne Messfehler/ aufzufallen
* Alice wählt die Polarisationen/ die Datenbits nach einem Muster (/zu wenig Entropie)
  + Wenn von Eve erkannt, kann Eve mithören, ohne Messfehler/ aufzufallen
* Zu kurzer Schlüssel
  + Durch Wiederholung eines zu kurzen Schlüssels kann Muster entstehen
  + Knackbar mit Brute-Force

Bob

* Bob und Eve wählen immer kontinuierlich die gleiche Polarisation (z.B. +) zum Messen
  + Alle Photonen, die Alice mit x polarisiert fallen beim Polarisationsvergleich heraus -> PreKey besteht nur aus Bits, deren Photonen mit + polarisiert wurden
  + Eve kennt somit auch alle relevanten Datenbits, ohne diese zu verändern

Alice oder Bob

* Alle/ zu viele PreKey-Bits werden zum Vergleich verwendet
  + -> FinalKey nicht lang genug/ nicht mehr vorhanden
* Keine/ zu wenige PreKey-Bits werden zum Vergleich verwendet
  + -> Mithören von Eve nicht erkennbar
* Polarisationen sind verschieden -> Benutzer erkennt sie als gleich bzw.  
  Polarisationen sind gleich –> Benutzer erkennt sie als verschieden
  + Beim händischen Vergleichen der Polarisationsbits von Alice und der Polarisationsbits von Bob werden zwei gleiche Bits als unterschiedliche bzw. zwei unterschiedliche als gleiche Bits erkannt
  + -> falscher PreKey entsteht
* Polarisationsreihenfolge wird geschickt, bevor Photonen gesendet werden
  + Nutzer erzeugt Polarisationen
  + Nutzer klickt Button ‚Polarisation senden‘
  + Nutzer klickt Button ‚Photonen senden‘ in „Alice“-Oberfläche