Binding to v6 or not

- draft-ietf-openpgp-pqc-02 binds PQ signatures to v6
- draft-ietf-openpgp-pqc-02 does not bind PQ encryption to v6
  - as to not impede the adoption of PQ encryption
  - should it?
I think it should bind to v6

- clear and concise messaging
- let PQ be a reason to switch to v6!
- binding PQ encryption subkeys to v4 certificates isn’t viable

Figure: https://tests.sequoia-pgp.org/#Mock_PQ_subkey
Encrypting to classical and PQ

- encrypt a message for an ECC recipient and PQ recipient
  - obviously losing the PQ safety
  - but maybe better than plaintext

- should that work?
- should that fail?
- who decides?
  - the spec?
  - the sender?