Distort TLS

Types of Changes

- Formatting Changes
- Cryptographic Changes
- Behavior Changes

- At what point does a new proof become required

Formatting Changes

- Remove legacy
- Switch to CBOR
- Kill Encrypted Extensions if not used
- Use compressed ECDH keys
- Rewrite all of the lists of values
  - Loses the new signature/hash formatting
- Re-encode array of one options

Possible formatting changes

- Finish removing record layer
- Remove extension structure to a fixed set

Cryptographic Changes

- Remove the random values
- Change to 64-bit finish values and other HMACs on the wire
- Allow for reference of signing key
  - Definitely not covered by current TLS evaluations.
  - Rejigger to include public key in transcript

Other Cryptographic Changes

- Remove binders on PSKs

Behavior Changes

- Change the default values in some places
  - Default certificate goes to RPK or reference
- Define a new reference certificate (and maybe some others)
- Change behavior of curves extension – omitted = the one I offered