TLS 1.3 is much better than TLS 1.2

✓ Only one round in the handshake (vs 2 with TLS 1.2)

✓ Faster (use of elliptic curves)

✓ Certificate is encrypted (better confidentiality)

✓ Protocol has been formally proven
(dos not prevent from implementation bugs)

The Signal Protocol