Preventing denial of service attacks on TLS handshakes

Client puzzle and exploration of other approaches

Problem

- TLS handshakes are fundamentally asymmetric in computational effort
- Seems to be actually exploited in practice

source on active attacks: https://www.youtube.com/watch?v=pBNMWvfL05g

Client puzzles

- Direct throttling of client request by requiring them to do calculations
- Nygren draft: https://datatracker.ietf.org/doc/html/draft-nygren-tls-client-puzzles-02
- Revival: https://github.com/tweedegolf/draft-TLS-client-puzzles

(submitted as I-D under draft-venhoek-tls-client-puzzles-00)

Alternate solutions

- Faster signatures (batching)
- Optimizing handshakes/packet handling
- Other suggestions?