- **`Extensibility`**: the modular design allows for protocol extensions and improvements without breaking existing implementations. New features can be negotiated during session establishment through capability flags.

6. References

[01] Chaum, D. (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, 24(2), 84-90. https://www.freehaven.net/anonbib/cache/chaum-mix.pdf

[02] Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). Anonymous Connections and Onion Routing. IEEE Journal on Selected Areas in Communications, 16(4), 482-494. https://www.onion-router.net/Publications/JSAC-1998.pdf

[03] Bradner, S. (1997). Key words for use in RFCs to Indicate Requirement Levels. IETF RFC 2119. https://datatracker.ietf.org/doc/html/rfc2119

[04] Danezis, G., & Goldberg, I. (2009). Sphinx: A Compact and Provably Secure Mix Format. 2009 30th IEEE Symposium on Security and Privacy, 262-277. https://cypherpunks.ca/ iang/pubs/Sphinx_Oakland09.pdf

[05] Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Lightning Network Whitepaper. https://lightning.network/lightning-network-paper.pdf

[06] Pfitzmann, A., & Köhntopp, M. (2001). Anonymity, Unobservability, and Pseudonymity—A Proposal for Terminology. In Designing Privacy Enhancing Technologies (pp. 1-9). Springer. https://www.freehaven.net/anonbib/cache/terminology.pdf

[07] Raymond, J. F. (2001). Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. In Designing Privacy Enhancing Technologies (pp. 10-29). Springer. https://www.freehaven.net/anonbib/cache/raymond-thesis.pdf