and Key Management Algorithm - Double Ratchet algorithm. The two encryption algorithms AES and ChaCha20 are widely accepted. It can be noted that RSA key exchange, DES cryptosystem, SHA-1 and MD5 hash functions are all depreciated. Among the mentioned algorithms ECDSA, EdDSA, ECDHE, X3DH, Double Ratchet algorithm are quantum unsafe while AES, ChaCha20 and SHA-256 are quantum safe.

REFERENCES

[1] *Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott, Thyla van der Merwe, "A Comprehensive Symbolic Analysis of TLS 1.3", CCS'17, pp. 1773-1788.*

[2] *"TLS 1.3 - Enhanced Performance, Hardened Security." [Online]. Available: https://www.cloudflare.com/learning-resources/tls-1-3/.*

[3] *"What You Need to Know About TLS 1.3." [Online]. Available:*

https://www.ssl.com/blogs/need-know-tls-1-3/

[4] *"Overview of TLS v1.3" by OWASP.*

[5] *"The X3DH Key Agreement Protocol." [Online]. Available: https://signal.org/docs/specifications/x3dh/.*

[6] *Julia Bobrysheva, Sergey Zapechnikov, "Post-Quantum Security of Messaging Protocols: Analysis of Double Ratcheting Algorithm", IEEE, 2020, pp. 2041 – 2044.*

[7] *"The Double Ratchet Algorithm." [Online]. Available: https://signal.org/docs/specifications/doubleratchet/.*

[8] *"The (Real) Internet Key Exchange." [Online]. Available: https://tools.ietf.org/html/draft-harkins-ikev3-00.*

[9] *"The Secure Shell (SSH) Transport Layer Protocol." [Online]. Available: https://tools.ietf.org/html/rfc4253.*

[10] *"Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification." [Online]. Available: https://tools.ietf.org/html/rfc8551.*

[11] *"What next in the world of post-quantum cryptography?" [Online]. Available: https://www.ericsson.com/en/blog/2020/3/post-quantum-cryptography-symmetric-asymmetric-algorithms.*