References

[1] M. R. Nosouhi, S. W. A. Shah, L. Pan, and R. Doss, "Bit flipping key encapsulation for the post-quantum era," *IEEE Access*, vol. 11, pp. 56 181–56 195, 2023, ISSN: 2169-3536. DOI: 10.1109/access.2023.3282928.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, Dec. 2018, ISBN: 9780429466335. DOI: 10.1201/9780429466335.

[3] N. Bindel, J. Brendel, M. Fischlin, B. Goncalves, and D. Stebila, *Hybrid key encapsulation mechanisms and authenticated key exchange*, Cryptology ePrint Archive, Paper 2018/903, Oct. 2018. DOI: 10.1007/978-3-030-25510-7_12. [Online]. Available: https://eprint.iacr.org/2018/903/.

[4] V. Lyubashevsky, *Basic lattice cryptography: The concepts behind kyber (ml-kem) and dilithium (ml-dsa)*, Cryptology ePrint Archive, Paper 2024/1287, Oct. 2024. [Online]. Available: https://eprint.iacr.org/2024/1287/.

[5] J. Katz, *Introduction to Modern Cryptography* (Chapman & Hall/CRC Cryptography and Network Security Series), Third edition. Boca Raton, FL: CRC Press, 2021, ISBN: 9781351133005.

[6] R. Wolf, *Quantum Key Distribution: An Introduction with Exercises* (Lecture Notes in Physics). Springer International Publishing, 2021, ISBN: 9783030739911. DOI: 10.1007/978-3-030-73991-1.

[7] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," *Journal of the ACM*, vol. 60, no. 6, pp. 1–35, Nov. 2013, ISSN: 1557-735X. DOI: 10.1145/2535925.

[8] P. Pessl, L. G. Bruinderink, and Y. Yarom, *To bliss-b or not to be - attacking strongswan's implementation of post-quantum signatures*, Cryptology ePrint Archive, Paper 2017/490, Aug. 2017. DOI: 10.1145/3133956.3134023. [Online]. Available: https://eprint.iacr.org/2017/490/.

[9] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, *Newhope without reconciliation*, Cryptology ePrint Archive, Paper 2016/1157, Nov. 2016. [Online]. Available: https://eprint.iacr.org/2016/1157/.

[10] R. Misoczki, J.-P. Tillich, N. Sendrier, and P. S. L. M. Barreto, "Mdpc-mceliece: New mceliece variants from moderate density parity-check codes," in *2013 IEEE International Symposium on Information Theory*, IEEE, Jul. 2013, pp. 2069–2073. DOI: 10.1109/isit.2013.6620590.

[11] E. Rescorla, "The transport layer security (tls) protocol version 1.3," Internet Engineering Task Force, Internet-Draft draft-ietf-tls-rfc8446bis-11, Sep. 2024. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8446bis/11/.

[12] A. O. Freier, P. Karlton, and P. C. Kocher, "The ssl protocol version 3.0," Internet Engineering Task Force, Internet-Draft draft-ietf-tls-ssl-version3-00, Nov. 1996. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-ssl-version3/00/.

[13] H. Ghafghazi, A. El Mougy, H. T. Mouftah, and C. Adams, "Security and privacy in lte-based public safety network," in *Wireless Public Safety Networks 2*. Elsevier, 2016, pp. 317–364, ISBN: 9781785480522. DOI: 10.1016/b978-1-78548-052-2.50011-6.