DAFTAR PUSTAKA

Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Miller, C., Moody, D., Peralta, R. dan Perlner, R., 2022, *Status report on the third round of the NIST post-quantum cryptography standardization process*, US Department of Commerce, NIST.

Chizhov, I.V. and Borodin, M.A., 2013, *The failure of McEliece PKC based on Reed-Muller codes*, IACR Cryptology ePrint Archive.

Cho, J., No, J.S., Lee, Y., Kim, Y.S. and Koo, Z., 2022, *Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature and Fast Verification for Post-Quantum Cryptography*, Cryptology ePrint Archive.

Cooperstein, B.N., 2015, *Advanced Linear Algebra*, CRC Press.

Courtois, N., Finiasz, M., dan Sendrier, N., 2001, *How to achieve a McEliece-based digital signature scheme*, Prociding Asiacrypt, vol. 2248, pp. 157-174.

Dumer, I., 2004, *Recursive decoding and its performance for low-rate Reed-Muller codes*, IEEE Transactions on Information Theory, vol. 50, no. 5, pp. 811-823.

Huffman, W. Cary., Pless, Vera., 2003, *Fundamental of Error Correcting Codes*, Cambridge University Press, New York.

Lee, Y., Lee, W., Kim, Y.-S. and No, J.-S., 2020, *Modified pqsigRM: RM Code-Based Signature Scheme*, IEEE Access, vol. 8, p. 177506-177518.

Lee, W., No, J.-S., and Kim, Y.-S., 2017, *Punctured Reed-Muller code-based McEliece cryptosystem*, IET Communications, vol. 11, no. 10, pp. 1543-1548.

Lee, W., Kim, Y.-S. and No, J.-S., 2017, *A new signature scheme based on punctured Reed-Muller code with random insertion*, arXiv preprint arXiv:1711.00159.

Ling, San., and Xing, Chaoping., 2004, *Coding Theory A First Course*, Cambridge University Press, New York.

McEliece, R.J., 1978, *A Public-Key Cryptosystem based on Algebraic Coding Theory*, Communications System Research Section.

Muller, D.E., 1954, *Application of Boolean Algebra to Switching Circuit Design and to Error Detection*, I.R.E Transactions on Electronic Computer, no. 3, pp. 6-12.

Reed,I., 1954, *A class of multiple-error-correcting codes and the decoding scheme*, IEEE Transaction on Information Theory, vol. 4, no. 4, pp. 38-49.

Roman, S., 2008, *Advanced Linear Algebra*, Springer Science & Business Media, LCC.

Sidelnikov, V.M., 1994, *A Public-Key Cryptosystem based on Binary Reed-Muller Codes*, Discrete Mathematics and Applications, vol.4, no.3, pp.191-207.

Sendrier, N., 1997, *On the dimension of the hull*, SIAM Journal on Discrete Mathematics, 10.2, pp 282-293.