# DAFTAR PUSTAKA

Adkins, W.A. and Weintraub, S.H., 2012, *Algebra: an approach via module theory*, Springer Science & Business Media.

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

Baena, J., Briaud, P., Cabarcas, D., Perlner, R., Smith-Tone, D. and Verbel, J., 2022, *Improving support-minors rank attacks: applications to GeMSS and Rainbow*, Annual International Cryptology Conference, pp. 376-405, Cham: Springer Nature Switzerland.

Casanova, A., Faugere, J.C., Macario-Rat, G., Patarin, J., Perret, L. and Ryckeghem, J., 2017, *GeMSS: a great multivariate short signature* Doctoral dissertation, UPMC-Paris 6 Sorbonne Universités, INRIA Paris Research Centre, MAMBA Team, F-75012, Paris, France, LIP6-Laboratoire d'Informatique de Paris 6.

Cooperstein, B., 2015, *Advanced linear algebra*, CRC Press.

Cox, D., Little, J. and OShea, D., 2013, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, Springer Science & Business Media.

Dummit, D.S. and Foote, R.M., 2004, *Abstract algebra*, Hoboken: Wiley.

Ding, J., Petzoldt, A., and Schmidt, D.S., 2020, *Multivariate cryptography*, Multivariate Public Key Cryptosystems, pp.7-23.

Faugere, J.C. and Joux, A., 2003, *Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases*, Annual International Cryptology Conference, pp. 44-60, Berlin, Heidelberg: Springer Berlin Heidelberg.

Horn, R.A. and Johnson, C.R., 2012, *Matrix analysis*, Cambridge university press.

Kipnis, A., Patarin, J. and Goubin, L., 1999, *Unbalanced oil and vinegar signature schemes*, International Conference on the Theory and Applications of Cryptographic Techniques, pp. 206-222, Berlin, Heidelberg: Springer Berlin Heidelberg.

Lidl, R. and Niederreiter, H., 1997, *Finite fields*, Cambridge university press.

Malik D.S., Mordeson J.M. and Sen M.K., 1997, *Fundamentals of Abstract Algebra*, McGraw-Hill.

Matsumoto, T. and Imai, H., 1988, *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*, Advances in Cryptology—EUROCRYPT'88: Workshop on the Theory and Application of Cryptographic Techniques Davos, Switzerland, May 25–27, 1988 Proceedings 7, pp. 419-453, Springer Berlin Heidelberg.

Øygarden, M., Smith-Tone, D. and Verbel, J., 2021, *On the effect of projection on rank attacks in multivariate cryptography*, Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings 12, pp. 98-113, Springer International Publishing.

Patarin, J., 1995, *Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88*, Advances in Cryptology—CRYPT0'95: 15th Annual International Cryptology Conference Santa Barbara, California, USA, August 27–31, 1995 Proceedings 15, pp. 248-261, Springer Berlin Heidelberg.

Patarin, J., 1996, *Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms*, International Conference on the Theory and Applications of Cryptographic Techniques, pp. 33-48, Berlin, Heidelberg: Springer Berlin Heidelberg.

Rodrıguez, B.G., 2023, *HPPC: Hidden Product of Polynomial Composition*, Cryptology ePrint Archive.

Roman, S., Axler, S., & Gehring, F. W., 2005, *Advanced linear algebra*, New York: Springer.

Shamir, A. and Kipnis, A., 1999, *Cryptanalysis of the HFE public key cryptosystem*, Advances in Cryptology, Proceedings of Crypto, vol. 99.

Shor, P.W., 1999, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM review, 41(2), pp.303-332.

Stinson, D. R., & Paterson, M., 2018, *Cryptography: theory and practice*, CRC press.

Steeb, W. H., & Shi, T. K., 1997, *Matrix calculus and Kronecker product with applications and C++ programs*, World Scientific.

Tao, C., Petzoldt, A., & Ding, J., 2020, *Improved key recovery of the hfev- signature scheme*, Cryptology ePrint Archive.

Wahyuni, S., Wijayanti, I.E., Yuwaningsih, D.A. and Hartanto, A.D., 2021, Teori ring dan modul, UGM PRESS.

Wolf, C., 2005, *Multivariate quadratic polynomials in public key cryptography*, Cryptology ePrint Archive.

Wolf, C. and Preneel, B., 2005, *Taxonomy of public key schemes based on the problem of multivariate quadratic equations*, Cryptology ePrint Archive.