Literaturverzeichnis

[1] M. W. Baldoni, C. Ciliberto, and G. M. P. Cattaneo. *Elementary Number Theory, Cryptography and Codes*. Springer Berlin Heidelberg, 2009.

[2] E. Berlekamp, R. McEliece, and H. van Tilborg. On the inherent intractability of certain coding problems (corresp.). *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.

[3] D. J. Bernstein, J. Buchmann, and E. Dahmen. Post-quantum cryptography.–2009. *DOI: https://doi. org/10.1007/978-3-540-88702-7*.

[4] T. A. Berson. Failure of the mceliece public-key cryptosystem under message-resend and related-message attack. In *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*, volume 1294 of *Lecture Notes in Computer Science*, pages 213–220. Springer, 1997.

[5] D. Y.-K. L. Dr. Lily Chen, Dr. Dustin Moody. Nist post-quantum cryptography, 2023.

[6] D. Engelbert, R. Overbeck, and A. Schmidt. A summary of mceliece-type cryptosystems and their security. *Journal of Mathematical Cryptology*, 1(2):151–199, 2007.

[7] D. J. B. et al. Classic mceliece - cryptosystem specification, design rationale, guide for security reviewers, guide for implementors, 2023.

[8] K. Fleming. Classic-mceliece-round3-official-comment.

[9] B. Friedrichs. *Kanalcodierung: Grundlagen und Anwendungen in modernen Kommunikationssystemen*. Springer-Verlag, 1996.

[10] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Annual international cryptology conference*, pages 537–554. Springer, 1999.

[11] B. für Sicherheit in der Informationstechnik (BSI). Kryptografie quantensicher gestalten. Technical report, Bundesamt für Sicherheit in der Informationstechnik (BSI), 53133 Bonn, 12 2021.

[12] V. Goppa. A new class of linear correcting codes, 1970.

[13] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge university press, 2010.

[14] S. Jordan. Quantum algorithm zoo, Last updated: June 26, 2022.

[15] Y. X. Li, R. Deng, and X. M. Wang. On the equivalence of mceliece's and niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory*, 40(1):271–273, 1994.

[16] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977.

[17] M. Marcus, T. Lange, and P. Schwabe. White paper on mceliece with binary goppa codes, 2019.

[18] R. McEliece. A public-key cryptosystem based on algebraic coding theory. the deep space network progress report, dsn pr 42–44, 1978.

[19] M. Mosca. Cybersecurity in an era with quantum computers: will we be ready? *IEEE Security & Privacy*, 16(5):38–41, 2018.

[20] R. Niebuhr. Critical attacks in code-based cryptography. *WEWoRC*, 2011:34, 2011.

[21] N. Patterson. The algebraic decoding of goppa codes. *IEEE Transactions on Information Theory*, 21(2):203–207, 1975.

[22] O. Pretzel. *Error-correcting codes and finite fields*. Oxford Applied Mathematics & Computing Science S. Clarendon Press, Oxford, England, Aug. 1992.

[23] M. Repka and P.-L. Cayrel. Cryptography based on error correcting codes. In *Advances in Information Security, Privacy, and Ethics*, pages 133–156. IGI Global.

[24] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[25] P. W. Shor. Progress in quantum algorithms. *Quantum information processing*, 3:5–13, 2004.

[26] H. Singh. Code based cryptography: Classic mceliece. *arXiv preprint arXiv:1907.12754*, 2019.

[27] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa. A method for solving key equation for decoding goppa codes. *Information and Control*, 27(1):87–99, 1975.

[28] F. K. Wilhelm, R. Steinwandt, B. Langenberg, P. J. Liebermann, A. Messinger, P. K. Schuhmacher, and A. Misra-Spieldenner. Status of quantum computer development. 2020.