

# INTRODUCTION TO QUANTUM-SAFE CRYPTOGRAPHY

Summer Graduate School, June 24–July 5, 2024  
IBM, Zürich

[1] **A basic course in linear algebra, for example:**

S. AXLER, *Linear algebra done right*, 4th ed., Undergraduate Texts in Mathematics, Springer, Cham, 2024, ISBN 978-3-031-41025-3; 978-3-031-41026-0. MR 4696768. Zbl 7795955. doi: 10.1007/978-3-031-41026-0. Open access.

[2] **A basic course in abstract algebra, for example:**

M. F. ATIYAH and I. G. MACDONALD, *Introduction to commutative algebra*, Addison-Wesley, Reading, MA, 1969. MR 242802. Zbl 0175.03601. doi: 10.1201/9780429493638.

[3] **Optional reading:**

S. D. GALBRAITH, *Mathematics of public key cryptography*, Cambridge University Press, Cambridge, UK, 2012, ISBN 978-1-107-01392-6. MR 2931758. Zbl 1238.94027. doi: 10.1017/CBO9781139012843. <https://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html>.