Protocols from the first lecture:

1. C. H. Bennett and G. Brassard (1984). Quantum cryptography: Public key distribution and coin tossing. Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India, Dec 9-12, 1984.
2. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical review letters, 67(6), 661.

Quantum composable security:

⋆ Tutorial given by Christopher Portmann: watch

1. Maurer, U., and Renner, R. (2011). Abstract cryptography. In Innovations in Computer Science.
2. Portmann, C., and Renner, R. (2014). Cryptographic security of quantum key distribution. arXiv preprint arXiv:1409.3525.

Quantum-proof extractors:

⋆ Tutorial given by Amnon Ta-Shma: watch

Some extractors are quantum-proof, e.g.,:

1. Tomamichel, M., Schaffner, C., Smith, A., and Renner, R. (2011). Leftover hashing against quantum side information. IEEE Transactions on Information Theory, 57(8), 5524-5535.
2. De, A., Portmann, C., Vidick, T., and Renner, R. (2012). Trevisan's extractor in the presence of quantum side information. SIAM Journal on Computing, 41(4), 915-940.

But not all

1. Gavinsky, D., Kempe, J., Kerenidis, I., Raz, R., and De Wolf, R. (2007, June). Exponential separations for one-way quantum communication complexity, with applications to cryptography. In Proceedings of the thirty-ninth annual ACM symposium on Theory of computing.

Reductions to IID:

1. Tomamichel, M., Colbeck, R., and Renner, R. (2009). A fully quantum asymptotic equipartition property. IEEE Transactions on information theory, 55(12), 5840-5847.
2. Dupuis, F., Fawzi, O., and Renner, R. (2020). Entropy accumulation. Communications in Mathematical Physics volume 379, pages 867-913.
3. Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R., and Vidick, T. (2018). Practical device-independent quantum cryptography via entropy accumulation. Nature communications, 9(1), 1-11.
4. Arnon-Friedman, R. (2020). Device-Independent Quantum Information Processing: A Simplified Analysis. Springer Nature.

Uncertainty relation:

1. Maassen, H., and Uffink, J. B. (1988). Generalized entropic uncertainty relations. Physical Review Letters, 60(12), 1103.
2. Berta, M., Christandl, M., Colbeck, R., Renes, J. M., and Renner, R. (2010). The uncertainty principle in the presence of quantum memory. Nature Physics, 6(9), 659-662.

Non-locality:

⋆ A recommended book: Scarani, V. (2019). Bell nonlocality. Oxford University Press.

The CHSH game:

1. Clauser, J. F., Horne, M. A., Shimony, A., and Holt, R. A. (1969). Proposed experiment to test local hidden-variable theories. Physical review letters, 23(15), 880.

Device-independent QKD:

⋆ Tutorial given by me: watch

1. Pironio, S., Acin, A., Brunner, N., Gisin, N., Massar, S., and Scarani, V. (2009). Device-independent quantum key distribution secure against collective attacks. New Journal of Physics, 11(4), 045021.

2. Arnon-Friedman, R., Renner, R., and Vidick, T. (2019). Simple and tight device-independent security proofs. SIAM Journal on Computing, 48(1), 181-225.

More:

⋆ A recent survey about QKD: S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi adn P. Wallden (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012-1236.

⋆ To learn more about quantum entropies: Tomamichel, M. (2015). Quantum information processing with finite resources: mathematical foundations (Vol. 5). Springer.