Additional Resources

Here, we will present some additional resources for further reading.

Resources 1 - SC: Recap of I2C
- Book on AES. Joan Daemen, Vincent Rijmen: The Design of Rijndael - The Advanced Encryption Standard (AES), Second Edition. Information Security and Cryptography, Springer 2020.

Resources 2 - SC: Disk Encryption and Message Authentication
- The theory-papers cited in the slides are rather old. For the proof ideas, refer to the lecture notes. If you're very interested in security proofs of such constructions, contact Bart Mennink for further references.
- On weak keys in polynomial-based MACs. Gordon Procter, Carlos Cid: On Weak Keys and Forgery Attacks Against Polynomial-Based MAC Schemes. FSE 2013: 287-304 (https://eprint.iacr.org/2013/144.pdf).
- Design of Poly1305. Daniel J. Bernstein: The Poly1305-AES Message-Authentication Code. FSE 2005: 32-49 (https://cr.yp.to/mac/poly1305-20050329.pdf).
- Of the assignments, the papers on PMAC (https://eprint.iacr.org/2001/027.pdf) and LightMAC (https://eprint.iacr.org/2016/190.pdf) are worth reading.

Resources 3 - SC: Authenticated Encryption
- GCM in general is possibly a nice read, though outdated. David A. McGrew, John Viega: The Security and Performance of the Galois/Counter Mode (GCM) of Operation. INDOCRYPT 2004: 343-355 (https://eprint.iacr.org/2004/193.pdf).
- The work of Böck et al. on nonce misuse. Hanno Böck, Aaron Zauner, Sean Devlin, Juraj Somorovsky, Philipp Jovanovic: Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS. WOOT 2016 (https://eprint.iacr.org/2016/475.pdf).
- A recent attack on the long-used OCB2. Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu, Bertram Poettering: Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality. CRYPTO (1) 2019: 3-31 (read instead: https://eprint.iacr.org/2018/1090.pdf).

Resources 4 - SC: Hash Functions and KDFs
- A nice generic second preimage attack on the Merkle-Damgaard construction, at that time demonstrating that its second preimage resistance was less than what was commonly believed. John Kelsey, Bruce Schneier: Second Preimages on n-Bit Hash Functions for Much Less than 2^n Work. EUROCRYPT 2005: 474-490 (https://link.springer.com/content/pdf/10.1007/11426639_28.pdf).
- Practical collision attack on SHA-1. Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, Yarik Markov: The First Collision for Full SHA-1. CRYPTO (1) 2017: 570-596 (https://eprint.iacr.org/2017/190.pdf).
- Improved preimage resistance of the sponge. Last year we observed that the preimage resistance of the sponge was actually higher than the bound that was proven 15 years ago and that was used in practice. Charlotte Lefevre, Bart Mennink: Tight Preimage Resistance of the Sponge Construction. CRYPTO (4) 2022: 185-204 (https://eprint.iacr.org/2022/734.pdf).

Resources 5 - SC: Keyed Sponges
- The Ascon sponge/duplex-based authenticated encryption scheme, recently selected as winner of

the NIST Lightweight Cryptography competition. Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer: Ascon v1.2: Lightweight Authenticated Encryption and Hashing. J. Cryptol. 34(3): 33 (2021) (https://link.springer.com/content/pdf/10.1007/s00145-021-09398-9.pdf).
- A detailed discussion of the duplex, its history, and the implications of its security. Bart Mennink: Understanding the Duplex and Its Security. IACR Trans. Symmetric Cryptol. 2023(2): 1-46 (2023) (https://eprint.iacr.org/2022/1340.pdf).
- An explanation of the ISAP authenticated encryption scheme, that is based on the sponge/duplex and offers leakage resilience. Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, Bart Mennink, Robert Primas, Thomas Unterluggauer: Isap v2.0. IACR Trans. Symmetric Cryptol. 2020(S1): 390-416 (2020) (https://tosc.iacr.org/index.php/ToSC/article/view/8625/8191).

Resources 6 - AC: Public Key Cryptography Basic Concepts
1. Eike Kiltz and John Malone-Lee, "A General Construction of IND-CCA2 Secure Public Key Encryption", IMACC 2003: 152-166
2. Eiichiro Fujisaki and Tatsuaki Okamoto, "How to Enhance the Security of Public-Key Encryption at Minimum Cost", Public Key Cryptography 1999: 53-68 (link: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=abf1e80e56cc7f384e2ed4f008a99f4405bbc41b)
3. Eiichiro Fujisaki and Tatsuaki Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Schemes", J. Cryptol. 26(1): 80-101 (2013) (link: https://link.springer.com/article/10.1007/s00145-011-9114-1)
4. Dennis Hofheinz, Kathrin Hövelmanns, Eike Kiltz, "A Modular Analysis of the Fujisaki-Okamoto Transformation", TCC 2017. Lecture Notes in Computer Science, vol 10677 (link: https://link.springer.com/chapter/10.1007/978-3-319-70500-2_12)
5. Alexander W. Dent, "A Designer’s Guide to KEMs", Cryptography and Coding 2003. Lecture Notes in Computer Science, vol 2898. Springer, Berlin, Heidelberg. (link: https://eprint.iacr.org/2002/174)