Readings for Lecture 23

Attached is:

- *Digital Cash: Chapter 6.4* [3].

- *Untraceable Off-line Cash in Wallet with Observers* [2].

- *Collusion-Secure Fingerprinting for Digital Data* [1].

References

[1] Dan Boneh and James Shaw. Collusion-secure fingerprinting for digital data. pages 452–465. Springer, 1995. Lecture Notes in Computer Science No. 963.

[2] Stefan Brands. Untraceable off-line cash in wallets with observers. In Douglas R. Stinson, editor, *Proc. CRYPTO 93*, pages 302–318. Springer, 1994. Lecture Notes in Computer Science No. 773.

[3] Bruce Schneier. *Applied Cryptography (Second Edition)*. John Wiley & Sons, 1996.