

Date:

02.11.23

Time:

4pm CEST

Reading materials:

- [Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing \(sections 2, 3\)](#)
- [Informal introduction to the Pedersen Commitment scheme on stackexchange](#)

Optional:

- [Zcash Protocol Specification NU5](#)