With all Mathematics preliminaries covered, we can now move to the next part of the book. This part is dedicated to the mathematical background required for Cryptography. Namely, we will cover essentials specified in Table 1.

Section	Topic	Key Concepts
??	Security Analysis	Advantage, negligible function, DL/CDH/DDH Assumptions
??	Elliptic Curves, ecpairing	Group of points on Elliptic Curve, Projective Coordinates, elliptic curve pairing
??	Commitment Schemes	Hash-based Commitments, Pedersen Commitments, KZG Commitments

Table 1: Topics covered in Part II

In the **??**, we consider the core object in the majority of modern zk-SNARK systems, the Elliptic Curves. Besides considering the definition and basics, we also describe the projective coordinates and the elliptic curve pairing operation. In the **??**, we consider the commitment schemes: hash-based, Pedersen, and KZG commitments. In the **??**, we consider the basics of security analysis, which, from the practical standpoint, is needed to read cryptographic papers and understand which security assumptions are used in the protocols and how authors typically describe them.