Finally, we consider the last part of the book. This part is dedicated to the zero-knowledge proofs, their applications, and the underlying theory. Namely, we will cover essentials specified in Table 1.

Section	Topic	Key Concepts
??	Introduction to Zero-Knowledge	Proof of Knowledge, Soundness, Relation and Language, P/NP Complexities, Fiat-Shamir Heuristic
??	Σ-Protocols	Shnorr Signatures, Okamoto Representation Protocol, Generalization
??	R1CS	Arithmetical Circuits, Why Rank-1, Matrix Form
??	QAP	Quadratic Arithmetic Program, Polynomial as Universal Encoders
??	Pairing-based SNARKs	Pinnochio and Groth16 Protocols; why such complicated expressions?
??	Circom	Programming R1CS in Circom, the language of zk-SNARKs
??	PlonK	FFT, Blinding, PlonKish Arithmetization
??	STARK	FRI, Hash-based proving system, Example

Table 1: Topics covered in Part III

While currently book features only Σ-proofs, zk-SNARKs, and STARKs, we plan to extend it with more topics in the future (such as Bulletproofs).