Motivation. Cryptography is wonderful. If you are holding this book, you are probably already know the significance of cryptography in the modern informational infrastructure: from classical standard protocols such as Transport Layer Security (TLS) to the more recent cryptographic advancements used in Blockchain technologies. This book is exactly about the latter.

In particular, as the book's name suggests, we consider the *zero-knowledge cryptography*, which is a cornerstone of numerous privacy-preserving protocols. However, in its current state, the zero-knowledge technology is *tremendously* hard to work with:

- The technology is relatively new, so there are almost no high-level abstractions that can be used to simplify the design of zero-knowledge protocols for regular developers.
- The technology is based on advanced mathematics, which is hard to understand without a proper background.
- The amount of available resources on the topic is surprisingly limited. What's more, the resources are very diverse: they are either (a) too high-level, which makes you understand what the protocol *should* do, but you still have no idea how to implement it, (b) or too low-level, consisting of numerous security proofs and obscure theorems with little practical implications. Note that in the latter case you typically still have no clue what was going on, unless you spend a significant amount of time studying the topic.

Of course, this book cannot solve all the aforementioned problems at once. However, we do hope that this book will serve as a complete, practical guide to most state-of-the-art techniques in zero-knowledge cryptography for practicing engineers. We gathered all the necessary information in one place, and tried to make it easy-to-follow, with a lot of examples and code snippets. Yet, we still try to preserve the mathematical rigor where suitable and necessary.

Who are we? We are *Distributed Lab* — a Ukrainian cryptography and engineering team focused on cryptography related projects (primarily in Bitcoin and EVM ecosystems). We have been working on numerous zero-knowledge solutions involving optimizing advanced algebraic system components, ranging from fast Groth16 RSA or 384-bit Brainpool ECDSA verification to PlonK circuits acceleration of BN254 elliptic curve operations and pairing. We are significantly contributing to the Bitcoin ecosystem and developing payment and social applications with the focus on privacy (e.g. *Rarimo*).

Who is this book for? This book does require basic background in Mathe-

matics. Of course, we will try to explain all the necessary concepts from scratch (such as basic number and group theory, security analysis), but this material is rather supplementary and is not the main focus of the book. That being said, you do not need Math PhD, but be prepared: the book is challenging.

How to use this book? The book is structured in the following way:

1. The first part of the book, consisting of sections from **??** to **??**, is dedicated to the theoretical background on Mathematics and Cryptography needed for understanding the zero-knowledge protocols. If you feel comfortable with polynomials, groups, elliptic curves and commitment schemes, you can skip this part.
2. The main part of the book starts from **??**, where we first define the zero-knowledge proofs and explain the basic concepts behind them. We then proceed to the more advanced topics, such as Sigma protocols (**??**), SNARKs (from **??** to **??**), and PlonK (**??**).