v1.0.0

Least Authority
PRIVACY MATTERS

序

月球数学手册 After more than a decade of intense and fast-paced research on zk-SNARKs by mathematicians and cryptographers around the globe, the field is now racing towards full maturity, and I believe that we can see first saturation effects to appear at the horizon. I hope this book will equip the reader with most of the basic knowledge needed to implement secure applications, and to tackle the vast literature in this remarkable field of research.

一系列讲座和笔记

The book arose from a set of lectures and notes I gave at the Zero Knowledge Summit –ZK0x02 & ZK0x03 in Berlin. On the one hand side it originated from the desire to collect the scattered information around the topic of zk-SNARKS and present them to an audience that does not have a strong background in cryptography. On the other hand side it serves as a labbook to collect and present insights into common misunderstandings, that the Least Authority audit team gathered throughout their audits of various zk-SNARK implementations. It should be considered a constant work-in-progress as we try to update it whenever we think new zk-SNARK technology becomes relevant in real world applications.

The book is intended to let illustrative examples drive the discussion and present the key ideas of all basic concepts relevant to the understanding of

zk-SNARKS with as little mathematics as possible. For those who are new to this topic, it is my hope that the book might be particularly useful as a first read and prelude to more complete or advanced expositions.

– Mirco Richter –