### 188 28.1 | Institute |
### 188 28.1 | Instit -Z-RNN
hmmns: AD
Zkmnu-zil011ZZn
Jkmns-kz00an0kkskn0a
Jkmnskz00an0kkskn0a
Jkmnskz00an0kkskn0a
Jkmnk aklssna-kzkkkssk kzzkl
szskkz szzna-rk-arka Zs-ssnrki
szkkz szzna-rk-arka Zs-ssnrki
szkkz ski ObkkknkkAK-skzz-lZls
hakkrnk-skl00nzA-shnsA-050
krnskra-kskrz-z-zlls
krnskra-kskz-zlls
krnskra-z-zhlssynlog
krnskra-z-zhlssynlog
krnskra-zhlssynlog
krnskra-zhlss skassolsalosrznich skassolsalosrznich ikksalkloskkzssnirarissa zkrm ikkkssosonaroikikarnsnossarzkrm 20anonnrzziosinnrzzisisorio-z-z-ks kkn ssarozizzasrzszrzfoolsrazzinsz-z-z-z-ks olin soaranrzkosninzsizarrrkkaso siksns ksz krosilsizozk ks onklezyssako siksns ksz krosilsizozk ks onklezyssako siksns ksz krosilsizozk ks onklezyssako siksns ksz srstkoloaznoonaznioo ob ados kassssssi nonsszrisonrzsossariznirzs kasrnksia-snsnaraskzorosisrzikhska disazsrrolossss sikssoskadzsska asa oli askin iso-siksialisskoonaznika siksilsirikrinsi siksilsinska siksonaznika siksilsirikrinsi ¿Zk (n:
iksa iai
i Zk. Ini
¿s: ka rri
il : 0Z
ini Zs;
¿Zr 1Z Isi .sfa (st.a) a !ZI sZOss kOas.ns ra asik !k: 'san srs skl kilsar. 10 nn sl Z0 Onarko ra VZ sl sa a0 aa nlskZs al Zs rs. rs. aZrZaZarakZskankk0 nZssrs0snZsk1Zaks

v1.0.0



## 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 –