

To my parents, Kalman and Ora Rosen

Foreword

Zero-knowledge proofs are fascinating and extremely useful constructs. Their fascinating nature is due to their seemingly contradictory definition; zero-knowledge proofs are convincing and yet yield nothing beyond the validity of the assertion being proved. Their applicability in the domain of cryptography is vast; they are typically used to force malicious parties to behave according to a predetermined protocol. In addition to their direct applicability in cryptography, zero-knowledge proofs serve as a good benchmark for the study of various problems regarding cryptographic protocols (e.g., “secure composition of protocols”).

A fundamental question regarding zero-knowledge protocols refers to the preservation of security (i.e., of the zero-knowledge feature) when many instances are executed concurrently, and in particular under a purely asynchronous model. The practical importance of this question, in the days of extensive Internet communication, seems clear. It turned out that this question is also very interesting from a theoretical point of view. In particular, this question served as a benchmark for the study of the security of concurrent executions of protocols and led to the development of techniques for coping with the problems that arise in that setting.

Protocols that remain zero-knowledge also when many instances are executed concurrently are called **concurrent zero-knowledge**, and the current book is devoted to their study. In view of the fact that the aforementioned generic application of zero-knowledge protocols relies on their existence for any NP-set, we focus on the construction of concurrent zero-knowledge for every NP-set. The book starts by establishing the mere existence of concurrent zero-knowledge protocols (for any NP-set). We stress that the mere existence of non-trivial concurrent zero-knowledge protocols was not clear for a couple of years, and was established by Richardson and Kilian (in the late 1990s). Once the existence of concurrent zero-knowledge protocols (for any NP-set) was established, the study turned to the complexity of such protocols, focusing on the round-complexity (which is arguably the most important complexity

measure). The bulk of the book is devoted to the presentation of the results of that study. The main results presented in this book are:

1. Under standard intractability assumptions, concurrent zero-knowledge proofs with *almost-logarithmically many rounds* do exist (for any NP-set). As with all prior work, this result is established using a “black-box simulator”.
2. Black-box simulators cannot establish the concurrent zero-knowledge property of non-trivial protocols having significantly *fewer than logarithmically many rounds*. Black-box simulators are the most natural way to establish the zero-knowledge feature of protocols, and until very recently they were (falsely) considered unavoidable (and so limitations concerning them were considered inherent to zero-knowledge itself).

Combined, these two results determine the round-complexity of concurrent zero-knowledge when restricted to black-box simulations. In doing so, these results make a significant contribution to the study of zero-knowledge and security of protocols at large.

We wish to stress that although we currently realize that “black-box zero-knowledge” is weaker than standard zero-knowledge, it is still important to determine the limits of “black-box” techniques. Firstly, asserting that some problem cannot be solved using “black-box” techniques means that, even in case it is solvable (by “non-black-box” techniques), this problem is inherently harder than others that can be solved using “black-box” techniques. Indeed, solutions that rely on “non-black-box” techniques tend to be more complex not only from a conceptual perspective but also in terms of the time and communication complexities of the resulting protocol. Furthermore, the latter tend to provide a lower level of security.

The focus of this book is on the study of concurrent zero-knowledge protocols. In addition, the book contains a brief introduction to zero-knowledge and a brief account of other developments in the study of zero-knowledge. The purpose of these two augmentations, written by me, is to provide an introduction to the basic concepts that underlie the main subject matter as well as a wider perspective on them.

Weizmann Institute of Science
April 2006

Oded Goldreich

Acknowledgements

I would like to express my deepest gratitude to Oded Goldreich and Moni Naor. Oded and Moni are very special individuals, and each of them has affected my scientific development in his own distinctive way.

I would like to thank Oded for making the writing and publication of this book possible. Oded has invested an unparalleled amount of time and effort to supply me with invaluable advice about technical issues, as well as on the way the results in this book should be presented. There is no doubt that Oded has had a significant impact both on my scientific taste and on my approach to research. For that and for his devotion I thank him very much.

I am deeply indebted to Moni for treating me as a peer from the first moment. The credit he has given me has greatly contributed to my self-confidence as a researcher. Moni has always been available to discuss scientific issues and has continuously provided me with extremely interesting ideas for research. I consider myself lucky for having spent so much time in the presence of someone as resourceful as Moni. I know that I have benefitted from it a lot.

I am most grateful to Ran Canetti, Cynthia Dwork, Shafi Goldwasser, Danny Harnik, Silvio Micali, Rafael Pass, Tal Rabin, Omer Reingold, Ronen Shaltiel and Salil Vadhan for their invaluable support. It would be hard to underestimate the contribution of their advice and encouragement to my development as a researcher.

The students and faculty members at the Weizmann Institute have taught me a great deal, and have made the Institute a great place to study in. Thanks to Adi Akavia, Boaz Barak, Itai Benjamini, Uri Feige, Tzvikia Hartman, Robi Krauthgamer, Michael Langberg, Yehuda Lindell, Kobbi Nissim, Eran Ofek, Benny Pinkas, Ran Raz, Yoav Rodeh, Adi Shamir and Udi Wieder.

I would like to thank my co-researchers to the results that make up some of the chapters in this book. Chapter 7 was done jointly with Ran Canetti, Joe Kilian and Erez Petrank [30]. Chapter 5 is joint with Manoj Prabhakaran and Amit Sahai [93]. I would especially like to mention Joe for his generosity and for contributing so many key ideas to the field of concurrent zero-knowledge.

Thanks also to Alex Healy, Jonathan Katz, Shien Jin Ong and Salil Vadhan for their feedback on the presentation of the results in this book.

Most importantly, I would like to thank the members of my family for their love and encouragement throughout the years. My parents Ora and Kalman, my brothers Erez and Oren, my wife Vered and my sons Yoav and Itamar. I wish to express the deepest love to Vered, Yoav and Itamar. Being in their presence is a wonderful experience and I consider it the greatest privilege of them all. Finally, thanks to Rivka and Yossi for their much appreciated help with raising the kids.

Harvard University
April 2006

Alon Rosen



<http://www.springer.com/978-3-540-32938-1>

Concurrent Zero-Knowledge
With Additional Background by Oded Goldreich
Rosen, A.
2006, XIV, 184 p., Hardcover
ISBN: 978-3-540-32938-1