# Information Security and Cryptography



More information about this series at http://www.springer.com/series/4752

Colin Boyd • Anish Mathuria • Douglas Stebila

# Protocols for Authentication and Key Establishment

Second Edition

Springer

Colin Boyd
Department of Information Security
and Communication Technology
Norwegian University of Science
and Technology
Trondheim, Norway

Anish Mathuria
Dhirubhai Ambani Institute
of Information and Communication
Technology (DA-IICT)
Gandhinagar, Gujarat, India

Douglas Stebila
Department of Combinatorics
and Optimization
University of Waterloo
Waterloo, ON, Canada

Originally published under: Boyd C. and Mathuria A.

ISSN 1619-7100 ISSN 2197-845X (electronic)
Information Security and Cryptography
ISBN 978-3-662-58145-2 ISBN 978-3-662-58146-9 (eBook)
https://doi.org/10.1007/978-3-662-58146-9

To the memory of my father
*Thou thy worldly task hast done*
*– CB*

To the memory of my grandmother
*– AM*

To my parents and teachers
*– DS*

# Preface

The first edition of this book was published in 2003. Inevitably, certain parts of the book became outdated quickly. At the same time new developments have continued apace, including new concrete protocols, new understanding of protocol security properties, and new cryptographic primitives and techniques which can be used in protocol design. Work on a new edition began as early as 2010, but even as it was being written its scope expanded. We are aware that some important protocols have been omitted, and that there are emerging areas which will see considerable activity in the near future (post-quantum secure protocols being one obvious example). However, we still hope that we have been able to capture most of the main developments that have occurred since the first edition.

This second edition has broadly the same purpose and scope as the first edition. We hope to provide a helpful reference for the expert while still being accessible to those newer to the topic, including those trying to obtain a broad overview of the field. In comparison with the first edition, there are three new chapters and all the other chapters (one renamed) have been extensively revised. The new book is around 50% larger with around 225 concrete protocols described and a bibliography with almost twice as many references. Some older material, which we deemed less relevant today, has been removed.

**Chapter 1** replaces the first two chapters from the first edition. The chapter is intended to provide the necessary background on cryptography, attack scenarios and protocol goals with an expanded coverage. The initial tutorial introduction has been moved to an appendix, while some parts of Chapter 2 from the first edition were removed as they seemed no longer relevant. An updated, but somewhat shortened, introduction to protocol verification is also included.

**Chapter 2** is the first completely new chapter, describing computational models for key exchange and authentication. The purpose of this chapter is not to provide a tutorial on how to read, let alone write, computational proofs, but rather to try to help readers understand what a computational proof provides and how to compare the many different computational models in use. In later chapters we

have freely made reference to the major computational models when discussing specific protocols and their security.

**Chapter 3** is an updated chapter covering protocols using shared key cryptography. This includes major updates on the status of the protocols in the ISO 9798-2 and 11770-2 standards.

**Chapter 4** is an updated chapter on protocols using public key cryptography. Again, this includes new developments of the ISO standard protocols, this time for the 9798-3 and 11770-3 protocols. Coverage of TLS is moved to the new Chap. 6 which is devoted to TLS.

**Chapter 5** on key agreement is, as in the first edition, the longest chapter. There is an amazing diversity of ideas in design of key agreement protocols, even in the simplest case covered in this chapter, which is limited to two-party protocols in the public key setting. Even though several older protocols from the first edition have been omitted, the revised chapter is now more than ten pages longer, illustrating that there are still many new developments occurring.

**Chapter 6** is a completely new chapter on the TLS protocol. As the most prominent key establishment protocol in use today, we believe it is more than justifiable to devote a chapter to TLS. The development of the protocol in the past 10 years, culminating in the new TLS 1.3 protocol, provides many lessons for those researching and implementing key establishment protocols.

**Chapter 7** is the third new chapter and is dedicated to ID-based protocols. While it gathers in some early ID-based protocols already included in the first edition, the coverage of pairing-based protocols forms the bulk of the chapter and is completely new.

**Chapter 8** is an updated chapter on password-based protocols. This is another topic where there has been a great deal of research activity since the first edition leading to a significant expansion in the chapter.

**Chapter 9** is an updated (and renamed) chapter on group key establishment. Although group protocols have a long history there has been much recent work to modernise the topic with stronger security properties and formal proofs.

**Appendix A** covers standards for key establishment and authentication protocols from various standards bodies, updated and expanded from the first edition.

**Appendix B** consists of a tutorial introduction to protocols for authentication and key establishment. This is unchanged from the corresponding section in the first edition, apart from some small notational revisions.

**Acknowledgements**

Many people have given their help and advice generously to help us to improve the quality of the book. Different people have reviewed and provided comment on various portions of the book. We thank them all for their generous spirit and are sincerely sorry if we have misinterpreted or forgotten any of their helpful advice. This list includes all those who we can remember; we hope not to have missed anyone.

| | | |
|---|---|---|
| Craig Costello | Sigurd Eskeland | Håkon Jacobsen |
| Tibor Jager | Chris Mitchell | Ruxandra Olimid |
| Kenneth Radke | SeongHan Shin | Berkant Ustaoglu |

In addition, Kazuki Yoneyama provided helpful answers to specific questions. We are solely responsible for all errors of fact, presentation style, or just plain typing errors that this book may have.

The team at Springer have been encouraging and helpful throughout. We would particularly like to thank Ronan Nugent for his unfailing confidence and quick action on all matters, even as we delayed time and again. Series editor Kenny Paterson provided enthusiastic and encouraging support.

CB would like to record his personal thanks to his family for bearing with denial of service during the seemingly interminable saga of the second edition. When the work started he was with Queensland University of Technology, particularly the School of Electrical Engineering and Computer Science. More recently he has been at the Norwegian University of Science and Technology in the department now called Information Security and Communication Technology. Both institutions have provided encouragement and resources to support this work.

AM would like to express his gratitude to his wife, Hemal, and daughter, Radhika, for their unfailing love, support, and patience. His work was carried out at the University of Massachusetts at Dartmouth and more recently at the Dhirubhai Ambani Institute of Information and Communication Technology. He would like to thank his colleagues at both of these institutions for their support and encouragement.

DS would like to thank CB and AM for inviting him to join them in updating the fine work they did in the first edition. This work has been carried out over his time at the Queensland University of Technology, McMaster University, and now the University of Waterloo, and colleagues at all of these were supportive of his work on this project.

This book was typeset in LaTeX on various platforms. The style for the protocols and attacks is adapted from Anselm Lingnau's float package.

Trondheim, Gandhinagar, Waterloo
January 2019

*Colin Boyd*
*Anish Mathuria*
*Douglas Stebila*

# Contents

# List of Protocols

# List of Attacks