CAMBRIDGE

Cambridge University Press
978-0-521-86485-5 - Quantum Cryptography and Secret-Key Distillation
Gilles Van Assche
Frontmatter
More information

# QUANTUM CRYPTOGRAPHY AND SECRET-KEY DISTILLATION

Quantum cryptography (or quantum key distribution) is a state-of-the-art technique that exploits the properties of quantum mechanics to guarantee the secure exchange of secret keys. This self-contained text introduces the principles and techniques of quantum cryptography, setting it in the wider context of cryptography and security, with specific focus on secret-key distillation.

The book starts with an overview chapter, progressing to classical cryptography, information theory (classical and quantum), and applications of quantum cryptography. The discussion moves to secret-key distillation, then privacy amplification and reconciliation techniques, concluding with the security principles of quantum cryptography. The author explains the physical implementation and security of these systems, and enables engineers to gauge the suitability of quantum cryptography for securing transmission in their particular application.

With its blend of fundamental theory, implementation techniques, and details of recent protocols, this book will be of interest to graduate students, researchers, and practitioners, in electrical engineering, physics, and computer science.

GILLES VAN ASSCHE received his Ph.D. in Applied Sciences from the Center for Quantum Information and Communication at the University of Brussels in 2005. He currently works in the Smartcard ICs Division at STMicroelectronics in Belgium. His research interests include quantum cryptography, classical cryptography, and information theory.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86485-5 - Quantum Cryptography and Secret-Key Distillation
Gilles Van Assche
Frontmatter
More information

# QUANTUM CRYPTOGRAPHY AND SECRET-KEY DISTILLATION

GILLES VAN ASSCHE

CAMBRIDGE
UNIVERSITY PRESS

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86485-5 - Quantum Cryptography and Secret-Key Distillation
Gilles Van Assche
Frontmatter
More information

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521864855

© Cambridge University Press 2006

This publication is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without
the written permission of Cambridge University Press.

First published 2006

Printed in the United Kingdom at the University Press, Cambridge

*A catalog record for this publication is available from the British Library*

ISBN-13 978-0-521-86485-5 hardback
ISBN-10 0-521-86485-2 hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86485-5 - Quantum Cryptography and Secret-Key Distillation
Gilles Van Assche
Frontmatter
More information

# Contents





© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86485-5 - Quantum Cryptography and Secret-Key Distillation
Gilles Van Assche
Frontmatter
More information





© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86485-5 - Quantum Cryptography and Secret-Key Distillation
Gilles Van Assche
Frontmatter
More information





© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86485-5 - Quantum Cryptography and Secret-Key Distillation
Gilles Van Assche
Frontmatter
More information

# Foreword

The distribution of secret keys through quantum means has certainly become the most mature application of quantum information science. Much has been written on quantum cryptography today, two decades after its inception by Gilles Brassard and Charles Bennett, and even longer after the pioneering work of Stephen Wiesner on non-counterfeitable quantum money which is often considered as the key to quantum cryptography. Quantum key distribution has gone from a bench-top experiment to a practical reality with products beginning to appear. As such, while there remain scientific challenges, the shift from basic science to engineering is underway. The wider interest by both the scientific and engineering community has raised the need for a fresh new perspective that addresses both.

Gilles Van Assche has taken up the challenge of approaching this exciting field from a non-traditional perspective, where classical cryptography and quantum mechanics are very closely intertwined. Most available papers on quantum cryptography suffer from being focused on one of these aspects alone, being written either by physicists or computer scientists. In contrast, probably as a consequence of his twofold background in engineering and physics, Gilles Van Assche has succeeded in writing a comprehensive monograph on this topic, which follows a very original view. It also reflects the types of challenge in this field – moving from basic science to engineering. His emphasis is on the classical procedures of authentication, reconciliation and privacy amplification as much as on the quantum mechanical basic concepts. Another noticeable feature of this book is that it provides detailed material on the very recent quantum cryptographic protocols using continuous variables, to which the author has personally contributed. This manuscript, which was originally written as a dissertation for the author's Ph.D. thesis, is excellent and, hence, was very appropriate to be turned into the present book.



© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86485-5 - Quantum Cryptography and Secret-Key Distillation
Gilles Van Assche
Frontmatter
More information



After an introduction to the basic notions of classical cryptography, in particular secret-key ciphers and authentication together with the concept of information-theoretic security, the tools of quantum information theory that are needed in the present context are outlined in the first chapters. The core of the book starts with Chapter 5, which makes a thorough description of quantum cryptosystems, from the theoretical concepts to the optical implementation. Chapter 6 considers the classical problem of distilling a secret key from the quantum data, a topic which is rarely treated to this depth in the current literature. The implementation of privacy amplification and reconciliation is illustrated more specifically in Chapters 7 and 8, while the case of continuous-variable reconciliation, which is the central contribution of Gilles Van Assche's thesis, is treated in Chapter 9. Then, the last chapters of the book study discrete-variable and continuous-variable quantum cryptographic protocols and analyze their security.

Gilles Van Assche has produced a remarkably self-contained book, which is accessible to newcomers to the field with a basic background in physical and computer sciences, as well as electrical engineering. Being fully up-to-date, this book will, at the same time, prove very useful to the scientists already involved in quantum cryptography research. With its science and engineering perspective, this book will undoubtedly become a reference in this field.

Nicolas J. Cerf
Professor
*Université Libre de Bruxelles*

Steven W. McLaughlin
Ken Byers Distinguished Professor
*Georgia Institute of Technology*

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86485-5 - Quantum Cryptography and Secret-Key Distillation
Gilles Van Assche
Frontmatter
More information

# Preface

This book aims at giving an introduction to the principles and techniques of quantum cryptography, including secret-key distillation, as well as some more advanced topics. As quantum cryptography is now becoming a practical reality with products available commercially, it is important to focus not only on the theory of quantum cryptography but also on practical issues. For instance, what kind of security does quantum cryptography offer? How can the raw key produced by quantum cryptography be efficiently processed to obtain a usable secret key? What can safely be done with this key? Many challenges remain before these questions can be answered in their full generality. Yet quantum cryptography is mature enough to make these questions relevant and worth discussing.

The content of this book is based on my Ph.D. thesis [174], which initially focused on continuous-variable quantum cryptography protocols. When I decided to write this book, it was essential to include discrete-variable protocols so as to make its coverage more balanced. In all cases, the continuous and discrete-variable protocols share many aspects in common, which makes it interesting to discuss about them both in the same manuscript.

Quantum cryptography is a multi-disciplinary subject and, in this respect, it may interest readers with different backgrounds. Cryptography, quantum physics and information theory are all necessary ingredients to make quantum cryptography work. The introductory material in each of these fields should make the book self-contained. If necessary, references are given for further readings.

### Structure of this book

The structure of this book is depicted in Fig. 0.1. Chapter 1 offers an overview of quantum cryptography and secret-key distillation. Chapters 2,



© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86485-5 - Quantum Cryptography and Secret-Key Distillation
Gilles Van Assche
Frontmatter
More information



3 and 4 give some aspects of classical cryptography, classical information theory and quantum information theory, respectively.

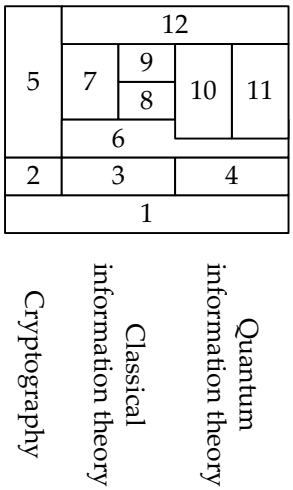


Fig. 0.1. Dependencies between chapters: a chapter depends on the chapter or chapters beneath. Block sizes are arbitrary.

Chapters 5–11 follow a top-down approach. First, Chapter 5 discusses quantum cryptography from an application point of view and macroscopically describes what services it provides and what are its prerequisites. Confidentiality requires a secret key, and Chapter 6 shows how to obtain one with secret-key distillation techniques. Secret-key distillation is further detailed in Chapters 7–9. Chapter 7 explains how to make the key secret using privacy amplification. This in turn requires the key to be error-free, and in this respect, the reconciliation techniques are detailed in Chapters 8 and 9. Then, the quantum sources of key elements to distill are described in Chapter 10 for discrete variables and in Chapter 11 for continuous variables.

Finally, Chapter 12 analyzes the security principles of quantum cryptography and revisits secret-key distillation from a quantum-physical perspective.

### Error reporting

If you find any error in this book, please do not hesitate to report it. You can find the contact information and an errata list on the web page: `http://gva.noekeon.org/QCandSKD/`.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-86485-5 - Quantum Cryptography and Secret-Key Distillation
Gilles Van Assche
Frontmatter
More information

# Acknowledgments

This book would not have been written without the support and help of many people. In particular, I would like to thank:

- Nicolas Cerf, my thesis supervisor, for his advice and support during the thesis;
- Steven McLaughlin, for his strong encouragements to take on this project and for his suggestions;
- the remaining members of the committee for their enthusiastic feedback: Daniel Baye, Michel Collard, Philippe Grangier, Olivier Markowitch, Serge Massar, and Louis Salvail;
- all the other researchers, with whom I worked or co-signed articles, or who reviewed parts of the text during the writing of this book: Matthieu Bloch, Jean Cardinal, Joan Daemen, Samuel Fiorini, Frédéric Grosshans, Sofyan Iblisdir, Marc Lévy, Patrick Navez, Kim-Chi Nguyen, Michaël Peeters, Rosa Tualle-Brouri, and Jérôme Wenger;
- Serge Van Criekingen for his thorough proof reading;
- my colleagues at the Center for Quantum Information and Communication for helpful discussion throughout the thesis;
- my colleagues at STMicroelectronics for their encouragements;
- my family and friends for their moral support;
- and last but not least, Céline for her encouragements and patience during the numerous hours I was busy working on this project.



© Cambridge University Press www.cambridge.org